

U.S. Department
of Transportation

**United States
Coast Guard**



SECURITY AWARENESS, TRAINING AND EDUCATION (SATE) PROGRAM



COMDTINST M5528.1



COMDTINST M5528.1

3 AUG 1993

COMMANDANT INSTRUCTION M5528.1

Subj: SECURITY AWARENESS, TRAINING AND EDUCATION PROGRAM

1. PURPOSE. To provide personnel with information and guidance for the implementation of the Coast Guard Security Awareness, Training and Education (SATE) Program.
2. ACTION. Area and district commanders, commanders of maintenance and logistics commands, commanding officers of headquarters units, and Commander, Coast Guard Activities Europe shall ensure compliance with the provisions of this instruction.
3. DIRECTIVE AFFECTED. The following is cancelled (superseded): CG-444-1, Security Education Manual.
4. DISCUSSION. A strong and continuing SATE Program is essential to instill security consciousness in all personnel and ensure a uniform interpretation and application of security standards. Any security program will prove ineffective unless supported by a comprehensive SATE Program. The goal is to develop fundamental habits of security to the point that proper discretion is automatically exercised in the performance of duties, and the protection of government assets (classified information, property, and personnel) becomes a natural element of every task.

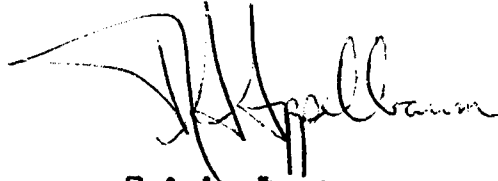
DISTRIBUTION - SDL No. 131

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	3	3	2		2	3	1	3	1	1		1	1	1	1	1	1	1	1		2	1				
B		8	26	2	2	2		10	2	2	1	1	1	10	2	2	2	10	1	2	2	1	1	1	1	2
C	3	2	1	3	3	3	1	1	1	1	3	1	2	1	2	1	3	1	2	1	1	1	1	1	1	1
D	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
E	1	1					1	1		1	1	1		1	1		1	1	1	1		1	1	1		
F	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1						
G	1	1																								
H																										

NON-STANDARD DISTRIBUTION:

3 AUG 1993

5. FORMS AVAILABILITY. Form CG-5274, Personnel Security Record, may be obtained from Supply Center Baltimore, using SN 7530-01-GF2-9820, U/I (PG).

A handwritten signature in black ink, appearing to read 'R. A. Appelbaum', with a stylized, sweeping flourish extending from the top left.

R. A. Appelbaum
Chief, Office of Law Enforcement and
Defense Operations

[illegible]

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION TO THE SECURITY AWARENESS, TRAINING AND EDUCATION (SATE) PROGRAM

A. General.....	1-1
B. Objective.....	1-1
C. Responsibilities.....	1-2
D. The Need for Security.....	1-2
E. Security Consciousness.....	1-3
F. Personal Recognition.....	1-3
G. Performance.....	1-4

CHAPTER 2. PROGRAM IMPLEMENTATION

A. General.....	2-1
B. Fact Finding.....	2-1
C. Resources.....	2-2
1. Briefings.....	2-2
2. Organizations/Associations.....	2-2
3. Posters.....	2-2
4. Audiovisuals.....	2-2
5. Literature.....	2-3
6. Office Products.....	2-3
7. Plan of the Day/Week and Newsletters.....	2-3
8. Security Awareness Day/Week/Month.....	2-3
D. How We Learn.....	2-4
1. Give the Learner an Interest in His/Her Work.....	2-4
2. Understanding What is Taught.....	2-5
E. Methods of Presentation.....	2-5
1. Lecture.....	2-5
2. Teaching Aids.....	2-6
3. Tests.....	2-6

Exhibit 2-1	Sources of Organizations/Associations.....	2-7
Exhibit 2-2	Sources for Security Posters.....	2-8
Exhibit 2-3	Audiovisuals.....	2-9
Exhibit 2-4	Literature.....	2-27
Exhibit 2-5	Test Questions.....	2-36

CHAPTER 3. SECURITY BRIEFINGS

A. Purpose.....	3-1
B. Responsibility.....	3-1
C. Types.....	3-1
1. Arrival Briefing.....	3-1
2. Access Briefing.....	3-1
3. Foreign Travel Briefing.....	3-1
4. Counterintelligence (CI) Awareness Briefing.....	3-1
5. Counterintelligence (CI) Awareness Debriefing.....	3-2
6. Annual Refresher Briefing.....	3-2
7. Transfer Briefing.....	3-2

8. Final Termination Briefing.....	3-2
D. Record of Briefings.....	3-3

Exhibit 3-1 Security Briefings Requirement Schedule.....	3-4
Exhibit 3-2 Arrival Briefing.....	3-6
Exhibit 3-3 Access Briefing.....	3-11
Exhibit 3-4 Foreign Travel Briefing.....	3-16
Exhibit 3-5 Counterintelligence (CI) Awareness Briefing.....	3-25
Exhibit 3-6 Counterintelligence (CI) Awareness Debriefing...	3-30
Exhibit 3-7 Transfer Briefing.....	3-32
Exhibit 3-8 Final Termination Briefing.....	3-34

CHAPTER 4. SECURITY TRAINING COURSES

A. Purpose.....	4-1
B. Priority Levels.....	4-1
C. Area and District Security Manager (SECMGR) Training.....	4-1
D. Additional Training.....	4-1

Exhibit 4-1 Security Manager Training.....	4-3
Exhibit 4-2 Security Related Training.....	4-6

Enclosures

- (1) Security Related References
- (2) Security Related Forms

CHAPTER 1. INTRODUCTION TO THE SECURITY AWARENESS, TRAINING AND EDUCATION (SATE) PROGRAM

A. General.

1. Security awareness is defined as a state of mind through which an individual is conscious of the existence of a security program and is persuaded that the program is relevant to his or her own behavior. This definition emphasizes that security awareness is part of a conscious process, i.e., it is a continuing attitude which can move an individual to specific actions.
2. Security awareness differs from education and training; although it is intimately related to both. In education, one acquires general knowledge about a subject or a field. The purpose of training is to develop specific skills or capabilities which the individual being trained will regularly use in the accomplishment of a task.
3. Simply stated, awareness seeks to solicit conscious attention, training seeks to develop skills (the how) and education seeks to impart generalized knowledge (the why).

B. Objective.

1. The objective of an effective SATE Program is to develop security awareness and acceptance by all personnel. Effective security is established when personnel recognize, understand and accept the need to protect government assets (classified information, property and personnel).
2. The overall program should be designed to:
 - (a) Advise personnel of the need to protect classified information and the damaging effects to the national security resulting from the compromise of classified information. Advise personnel of their responsibility to report administrative security discrepancies and possible compromises, and the disciplinary actions that may result.
 - (b) Indoctrinate personnel in the basic concepts of classification, downgrading and declassification. Alert personnel to the strict prohibition on improper use and abuse of the system.
 - (c) Advise personnel of the techniques employed by foreign intelligence services and criminal elements in attempting to obtain classified/sensitive law enforcement information and their responsibility for reporting such attempts.

- (d) Advise personnel of the hazards involved and the strict prohibition against discussing classified information over non-secure telephones or in the presence of unauthorized persons.
 - (e) Advise personnel of the need to protect government property and to report missing, lost or stolen government property.
 - (f) Advise personnel of their responsibility to report any adverse or questionable information that indicates an individual no longer meets the criteria for access to classified information.
 - (g) Indoctrinate personnel in the principles of Operations Security (OPSEC), including identification of vulnerabilities in their operations and the appropriate countermeasures to protect them.
3. The SATE Program must overcome the assumption by personnel that they need not be concerned with security unless they work with classified material or in a restricted area. The program must impress upon them that they are vital elements in the success of the program and a locked gate or secure container does not constitute an end in itself, but is merely another element in the overall security program.

C. Responsibilities.

- 1. Commandant (G-OIS-2) is designated as the Program Manager for the SATE Program, and is responsible for the development of Coast Guard-wide SATE policy, procedures and standards.
- 2. Security is an individual responsibility. Each employee has a direct, immediate, legal and moral responsibility for the proper protection of government assets. Regulations by themselves do not guarantee adequate security, but serve only as the basic guidelines within which we must operate to accomplish our security goals.

D. The Need for Security.

- 1. Recent world events have forced us to focus on the fact that all nations, no matter how friendly, collect strategic information concerning other countries. The threat to military and civilian personnel by foreign intelligence services may be changing but the risks remain the same. Military and civilian personnel are now, more than ever, meeting and communicating with foreign nationals from all over the world. More official visits are encouraged and anticipated.

2. Drastic changes in the world political structure pose new concerns. Continual struggles for nationalistic, religious and ethnic identities have significantly increased the risk of political violence. There is a growing division of the "haves" and "have-nots". The "have-nots" are becoming more aggressive, more militant, and more criminal in their efforts to "have".
3. We must be aware of the threat to our law enforcement missions. The adversary is monitoring our activities in order to circumvent our efforts. They are exploiting weaknesses in our operations security.
4. The SATE Program must be concerned with physical measures designed to prevent criminal acts; and counterintelligence measures designed to provide security for classified and sensitive information. Generating security awareness through education and training is considered one of the principal means of accomplishing this objective.

E. Security Consciousness. The intangible sense of self-responsibility, the trait which dispels carelessness, ignorance, or plain indifference, is "security consciousness". The degree of security consciousness is dependent upon how well we keep this awareness alive in each individual employee's mind. Not just a few minutes a day, but 24 hours a day, both on and off the job. Effective security can only exist in an environment where all personnel accept security responsibility with a confidence born of knowledge. The old cliché about security being everybody's business may have lost its punch (due to over-repetition or misuse) as the quick and easy answer to solve security problems without spelling out the HOW and WHY. Consequently, it is essential that personnel possess the knowledge and understanding of existing security regulations; HOW, WHEN and with WHOM to discuss classified information; and the duty to report security violations or problems. Only then have we achieved the desired goal of understanding - that is the WHY of security.

F. Personal Recognition. Another important facet to the SATE Program is coupled with adequate leadership and communication, achieved through personal recognition. If we take the time and effort to recognize an individual who has either done an outstanding security job or rendered some other contribution to the program, such recognition will effectively "sell" security to others. A letter of appreciation or commendation from the commanding officer, an article or notice in the Plan of the Day/Week or newsletter, security cartoon/poster contest, etc. is certain to stimulate wide interest.

- G. Performance. Job performance, as it relates to security, is affected by environment (e.g., equipment, tools, location); incentive motivation (e.g., feedback, policy, reward, recognition); and skills, knowledge (e.g., on-the-job training, resident training, job aides). To ensure a high level of job performance, we must address each of these critical areas. For additional information on performance problem solving and training development, refer to COMDTINST 1550.9, Management of the Coast Guard Training Program, or consult with Commandant (G-PRF).

CHAPTER 2. PROGRAM IMPLEMENTATION

A. General. When confronted with the requirement to formulate a Security Awareness, Training and Education (SATE) Program, many security personnel may find this task complex. This manual provides suggested techniques that will assist personnel in developing a successful SATE Program.

B. Fact Finding.

1. In order to plan and conduct an effective SATE Program, certain fundamental facts (information) must be obtained. These facts include information on existing security attitudes, problems, and requirements and may be best accomplished by an evaluation of the following:
 - (a) The levels and quantity of classified information handled by the unit and the total number of personnel with security clearances.
 - (b) The number, types and trends of security violations, possible compromises of classified information, and losses of government property.
 - (c) Any unique security problems/deficiencies.
 - (d) Informal evaluation of security plans and procedures, and review of security checklists.
 - (e) Review of vulnerabilities and criminal statistical data.
 - (f) Any problems, concerns and recommendations of personnel solicited through formal or informal discussion. The Security Outbrief Questionnaire in Exhibit 3-7 may be used for this purpose.
 - (g) The state of security awareness and the degree to which personnel understand and accept existing security regulations.
 - (h) Facilities and resources available (space, services, audiovisual equipment/aids, capabilities to produce material, etc.)
2. Is there a good indication about what personnel know, or more importantly, what they don't know? Don't take for granted that everyone is familiar with what a security professional would consider the basics. Get out and talk to people. Ask them what they are interested in knowing more about.
3. A review and evaluation of these findings will assist personnel in determining trends of strengths and

weaknesses - thus establishing the security goal. The goals established should be realistic, taking into account constraints upon time and resources.

C. Resources. Many resources are available to support the SATE Program. Included in this manual are suggestions and ideas, since "canned" material is valuable only to the extent that it is tailored to meet the specific needs of the unit. Security needs of the unit may vary depending on mission, size, location, composition, etc. This material may or may not contain specific security task information. If it directs the attention toward security content available elsewhere (in formal training materials) and generates approval or support of the main security objective, it will be effective. The techniques which have been used and are generally available include:

1. Briefings. Security briefings will essentially involve presentations in which attendance may range from a single individual to a large number of personnel. Chapter 3 provides extensive information on the required briefings and samples of briefing outlines.
2. Organizations/Associations. These sources can provide a wealth of information and security-related services. Some may provide (free or at a nominal cost) pamphlets, audiovisual programs and aids, and other commercially available security training material. Exhibit 2-1 lists a sampling of suggested sources.
3. Posters.
 - (a) Carefully chosen posters can be very effective. The old saying that "a picture is worth a thousand words" may be shopworn but it's true. Posters are only reminders. They should not be used to teach; they should be designed to reinforce security objectives and stimulate memory.
 - (b) Selecting the right posters and displaying them properly requires planning. A poorly selected subject or improperly placed poster might as well not be displayed at all. Select locations where they can be seen at eye level by the maximum number of people, e.g., cafeterias, water fountains, coffee messes, at the head of stairways, smoking areas, or other high traffic areas. Posters should be fresh, clean, and rotated frequently.
 - (c) Exhibit 2-2 lists a sampling of suggested sources for security posters.
4. Audiovisuals. Audiovisual program material can play a vital role in the SATE program. They should be used as

an aid to training, not as a replacement or stand alone. A careful selection should be made to ensure that the objective is met and the information is integrated into other material presented. Choose a program of proper length. Most last 15 minutes to an hour; however, the shorter the better. Audiovisual programs should be screened prior to viewing by the intended audience. Exhibit 2-3 lists a sampling of suggested sources and types of audiovisual programs.

5. Literature. This type of written material can be of value in expanding your knowledge and illustrating the need for security. Exhibit 2-4 lists a sampling of suggested books and publications which are available from libraries, bookstores, publishers, etc.
6. Office Products. Security slogans may be applied to a number of colorful and customized office products and objects, e.g., calendars, key chains, post-it-notes, pens, pencils, coasters, magnets, decals, rulers, etc. They serve as constant reminders and promote security awareness. These items are commercially available from local advertising companies.
7. Plan of the Day/Week and Newsletters. Most units publish some means of providing official and unofficial information to all hands. Security articles, cartoons, tips, puzzles, slogans, reminders, etc. may be included in these issues. They are a means of stimulating security awareness through the emphasis of key points. Topics may address portions of certain security requirements, changes in procedures, specific problem areas, etc. Local graphic art/design companies can provide clip art, designs, logos, etc. to support this type of printed material.
8. Security Awareness Day/Week/Month. This may require a bit of planning, but the results are well worth the effort. A designated day, week, or month will enhance security awareness and provide a timeframe for holding the required security briefings. The methods employed are only limited by the imagination and creativity of unit and security personnel. The following suggestions and ideas may be used:
 - (a) Advertise the designated period via a unit instruction and/or distribute flyers to spark interest.
 - (b) Provide handouts, pamphlets, etc. on various topics, e.g., crime prevention, anti-terrorism, classification markings, classified material control duties, etc.

- (c) Hold required annual refresher briefings and any applicable special briefings (foreign travel, counterintelligence, etc.).
- (d) Invite guest speakers from other government agencies and local police departments for optional briefings. Cognizant security managers (SECMGRs) may also be included.
- (e) Hold optional "lunch and learn" seminars.
- (f) Hold an optional "brown bag theater" and serve popcorn! Invite personnel to bring their lunch and watch a security video tape.
- (g) Hold a poster/cartoon contest.
- (h) Invite "McGruff", the Crime Prevention Dog. Provide kid identification kits (fingerprint cards, photographs, safety tips, etc.) to parents.
- (i) Use this timeframe to conduct inventories and purge classified holdings, conduct emergency destruction drills, verify government property listings, etc.

D. How We Learn. Learning begins when we see, hear, feel, smell, or taste something. All of the experiences of the senses make impressions on our minds. Seeing and hearing are the senses most often used in learning. Since impression is the first step in learning, an instructor should be able to understand how the audience can be given strong impressions. Most of our impressions come through the eyes. The printed page of a book or newspaper, the picture on a screen, writing on a blackboard, chart, or diagram, a sample handout - these are strong impressions because we can see them. If what we see is clear and vivid, we learn more effectively. Hearing is also important in our impressions. The loud enough, clear enough, understandable voice of the instructor is essential to understanding what is seen.

1. Give the Learner an Interest in His/Her Work. If we can give the audience the urge to want to learn, our job is greatly simplified. Attempt to instill an incentive in the minds of the individuals that will make them want to learn. Threatening them with penalties for failure to follow instructions, rules, etc. is not going to promote interest. In selling security, strive for:

- (a) Satisfaction of job well done.
- (b) Patriotism.
- (c) Self-protection.

- (d) Other objectives that will "reach" the individual.

2. Understanding What is Taught.

- (a) It is fine to say that the first page of a classified document will be classified as high as the highest category contained or that once you leave your job you should forget about your work and not talk about it. But why? Because if the person understands the purpose or meaning of what he or she is to do and the possible results of their failure to follow through, he or she is more likely to use the knowledge that is being presented.
- (b) Understanding, sometimes, is more easily obtained through "doing". Whenever possible, the learners should actually operate a safe combination, fill out a receipt, or prepare a document for transmission, etc. Nothing is better than actual experience. Take advantage of it at every opportunity.

E. Methods of Presentation.

1. Lecture. The lecture is a common method of security training. However, the lecture method alone is probably the least effective means of motivating learning, because it is one-way communication. While delivery is extremely important, regardless of how effective a speaker may be, the learning results will often be marginal unless this method is coupled with other techniques. This is because, with the pure lecture, the learner is placed in a passive role, can refuse to listen, think of something else besides the subject matter, or even go to sleep. Because of such limitations, other learning methods should be combined with the lecture, such as learner involvement. Such involvement can be achieved by soliciting questions or comments from the audience, distributing outlines, handouts, etc. The lecture method requires careful planning. The following steps may aid in the planning stages:

- (a) Decide exactly what points need to be covered.
- (b) Check reference material available on these points in other regulations, security briefs, etc.
- (c) Arrange the material systematically. Usually this will cover what, when, why, how, and possibly who.
- (d) Jot down the points and the material intended to be covered. A list or outline on a card or slip of paper is easy to glance at while speaking. Do not write out entire sentences and paragraphs or you will find yourself reading instead of talking.

- (e) Rehearse the talk several times to get used to it. If an important idea is omitted, put a reminder in the outline. Time yourself to know just how long the lecture will take.
2. Teaching Aids. Aids such as charts, graphs, chalkboards, easel charts, or slides can be utilized effectively to capture and keep the learner's attention. To be effective, the subject matter, the instructor, the learners, and the learning vehicles must be closely integrated with the aids being used. If not, the aids may distract and direct attention away from the subject matter. Common problems that detract from effectiveness are visual aids that are too small, too complicated, too garbled, or presented in an area or environment where the conditions make it difficult for the audience to comprehend.
3. Tests. Often overlooked as a teaching aid is the use of tests. Tests serve many purposes. Not only do they indicate extent of knowledge, but reviewing the test questions also imparts additional knowledge. Tests should be corrected (or self-corrected) and discussed with the individual immediately upon completion to maximize its benefits. Tests are also a means of measuring results in determining where the briefing has been effective and where teaching methods can be improved. Exhibit 2-5 lists a sampling of suggested test questions.

EXHIBIT 2-1

SOURCES OF ORGANIZATIONS/ASSOCIATIONS

Listed below is a compilation of suggested sources of various organizations and associations for security related assistance, products and services; it is not a complete list. The Coast Guard has not evaluated each source/product and makes no endorsement as to quality or suitability.

Department of Defense Security Institute
Defense General Supply Center
8000 Jefferson Davis Highway
Richmond, VA 23297-5091
(804) 279-4223

American Society for Industrial Security
1655 North Fort Myer Drive, Suite 1200
Arlington, VA 22209
(703) 522-5800

National Classification Management Society
6116 Roseland Drive
Rockville, MD 20852
(301) 231-9191

Interagency OPSEC Support Staff
6411 Ivy Lane, Suite 400
Greenbelt, MD 20770-1405
(301) 982-0323

American Association of Retired Persons
601 E. Street N.W.
Washington, DC 20049
(202) 434-2277

National Crime Prevention Council
1700 K. Street N.W., 2nd Floor, Room 3817
Washington, DC 20006
(202) 466-6272

Information Security Oversight Office
750 17th Street N.W., Suite 530
Washington, DC 20006
(202) 634-6122

National Computer Security Association
10 South Courthouse Avenue
Carlisle, PA 17013
(717) 258-1816

NOTE: Local law enforcement agencies and police departments can also assist in the security awareness, training and education effort.

EXHIBIT 2-2

SOURCES FOR SECURITY POSTERS

Listed below is a compilation of suggested sources for security posters; it is not a complete list. The Coast Guard has not evaluated each source/product and makes no endorsement as to quality or suitability.

The Network

National Business Crime Information Network
6649 Peachtree Industrial Boulevard, Suite J
Norcross, GA 30092
(800) 241-5689

American Council for Drug Education
204 Monroe Street
Rockville, MD 20850
(800) 488-3784

Performance Resource Press, Inc.
1863 Technology Drive
Troy, MI 48083
(313) 588-7733

Motivation Productions, Inc.
1475 N. Broadway, Suite 420
Walnut Creek, CA 94596
(415) 934-1061

The BUARTS Company
PO Box 583
Manhasset, NY 11030
(516) 627-8947

Incentive Marketing
PO Box 91929
Santa Barbara, CA 93190
(805) 962-4221

Medeco Security Locks, Inc.
PO Box 3075
Salem, VA 24153
(703) 380-5000

Defense Mapping Agency, HTC - Security Office
6500 Brooks Lane
Washington, DC 20315-0030

American Forces Information Service
Department of Defense
601 N. Fairfax Street, Room 312
Alexandria, VA 22314-2007

National Security Agency M54 (M56)
9800 Savage Road
Fort George G. Meade, MD 20755-6000

EXHIBIT 2-3

AUDIOVISUALS

Listed in this Exhibit is a compilation of audiovisual programs, compiled from the Army, Navy, Air Force, commercial vendors and other government agencies; it is not a complete list. The Coast Guard has not evaluated each source/product and makes no endorsement as to quality or suitability.

Note carefully the medium (videocassette, film, etc.), the source and whether it is available for loan or sale. Department of Defense products are available for loan at no cost. Commercially produced material is usually available for sale or rent; prices may be obtained directly from the vendor.

Copies of proprietary audiovisual productions may be protected under specific copyright laws and procurement conditions. Unauthorized use or reproduction may be copyright infringement. The U.S. Government and its employees have no general exemption from copyright infringement liability. An infringing user may be personally liable for monetary damages. If in doubt, contact your local procurement and/or legal authorities.

Each entry begins with the program title (in alphabetical order under each subject heading), date, length, medium, classification, source (with identification number) and summary. Some of this information is coded, as explained below.

CODES USED IN THIS LISTING:

MEDIUM: MP Motion Picture Film
VC Videocassette (VHS 1/2") (U-MATIC 3/4") (BETA)
ST Slides with cassette tape recording

CLASS: U Unclassified
C Confidential
S Secret
FOUO For Official Use Only

SOURCE: DA Army
DF Air Force
DN Navy
NCIS Naval Criminal Investigative Service
Other commercial vendors/government agencies

ARMY (DA) - Army products may be borrowed from the closest Army base Visual Information Library nearest you. If the product is not available, contact:

Joint Visual Information Activity
Warehouse 3, Bay 3
11 Midway Road
Tobyhanna Army Depot, PA 18466-5102
(717) 894-7941

AIR FORCE (DF) - Air Force products may be borrowed from the closest Air Force base Visual Information Library nearest you. If the product is not available, contact:

Air Force Central Visual Information Library
AFMEC-DOLD
106th Street, Bldg. 248
Norton Air Force Base, CA 92409-5996
(909) 382-2280

NAVY (DN) - Navy products may be borrowed from one of the Naval Education and Training Support Centers:

East of the Mississippi:

Commanding Officer
Naval Education and Training Support Center, Atlantic
9370 Decatur Avenue, Code N-5
Norfolk, VA 23511-34993499
(804) 444-1468/4011

West of the Mississippi:

Commanding Officer
Naval Education and Training Support Center, Pacific
921 W. Broadway, Code N53
San Diego, CA 92132-5105
(619) 532-1359/1360/1361

NCIS Navy crime prevention products may be borrowed from:

Naval Criminal Investigative Service - Code 24
Washington Navy Yard, Bldg. 111
Washington, DC 20388-5380
(202) 433-9136

GENERAL

ENFORCING SECURITY RULES

DATE: LENGTH: 17 min. MEDIUM: VC 1/2" CLASS: U
SOURCE: Coronet/MTI Film & Video, 108 Wilmet Road, Deerfield, IL 60015-5196,
(800) 621-2131
SUMMARY: Shows how to get people to understand the "WHY" of security rules.

SAFES, LOCKS AND VIDEOTAPES

DATE: 1991 LENGTH: 12 min. MEDIUM: VC CLASS: U
SOURCE: FilmComm, 641 North Avenue, Glendale Heights, IL 60139, (708) 790-3300,
or Pro Star International, P.O. Box 21526, Salt Lake City, UT 84121,
(800) 775-0761
SUMMARY: Discusses the different GSA containers and locks; container labels; how to inspect a container and lock; and how to change a combination.

ESPIONAGE AND COUNTERINTELLIGENCE

BEST KEPT SECRETS

DATE: LENGTH: 40 min. MEDIUM: VC, ID M56 1001 CLASS: U
SOURCE: National Security Agency (M56), Fort Meade, MD 20755-6000, (301) 688-6535
SUMMARY: TV Station WBAL, Baltimore, produced this five part series on the presence of hostile agents in the Baltimore-Washington area. It includes interviews with FBI Agents, Soviet defectors, and double agents, who highlight recruitment techniques and vulnerabilities of cleared U.S. personnel.

CARGO SECURITY AND TRANSPORTATION

DATE: 1984 LENGTH: 11 min. MEDIUM: VC 3/4" CLASS: U
SOURCE: DA: 701731
SUMMARY: Demonstrates why special physical security is required during transportation of classified and sensitive cargo. Presents procedures necessary for safe and secure transport from the origin transportation office to the destination transportation office.

COUNTERINTELLIGENCE AWARENESS BRIEF

DATE: 1990 LENGTH: 26 min. MEDIUM: VC 1/2" CLASS: U
SOURCE: DN: 804961
SUMMARY: Provides facts about the espionage threat from foreign intelligence services. Examines the extent and duration of various espionage threats by foreign governments trying to recruit Americans.

DARK SIDE OF ESPIONAGE

DATE: 1988 LENGTH: 15 min. MEDIUM: VC 3/4" 1/2" CLASS: U
SOURCE: FilmComm, 641 North Avenue, Glendale Heights, IL 60139, (708) 790-3300
SUMMARY: The objective is to increase the awareness of the hostile intelligence threat and its personal consequences. Christopher Boyce speaks directly to anyone who might consider committing espionage - now or in the future.

DECADE OF TRAITORS

DATE: LENGTH: 21 min. MEDIUM: VC 1/2" CLASS: U
SOURCE: National Security Agency (M56), Fort Meade, MD 20755-6000, (301) 688-6535
SUMMARY: Discusses recent espionage cases.

EAVESDROPPING

DATE: 1980 LENGTH: 22 min. MEDIUM: VC 3/4" 1/2" CLASS: U
SOURCE: Lockheed Missiles & Space Co., P.O. Box 3504, Attn: Security Training, 0/27-33 B509 Fac5, Sunnyvale, CA 94088-3504, (408) 742-4321
SUMMARY: Hostile intelligence threat briefing with emphasis on eavesdropping and listening devices.

ESPIONAGE ALERT

DATE: 1990 LENGTH: 16 min. MEDIUM: VC CLASS: U
SOURCE: FilmComm, 641 North Avenue, Glendale Heights, IL 60139, (708) 790-3300
SUMMARY: Tips on how to prevent espionage (80% is preventable). Summaries of four major spy cases.

ESPIONAGE 2000

DATE: 1990 LENGTH: 32 min. MEDIUM: VC CLASS: U
SOURCE: FilmComm, 641 North Avenue, Glendale Heights, IL 60139, (708) 790-3300
SUMMARY: An up-to-date foreign intelligence threat briefing that features many of the leading decision makers in government and industry.

FOREIGN INTELLIGENCE COLLECTION THREAT

DATE: 1987 LENGTH: 30 min. MEDIUM: VC 1/2" 3/4" BETA CLASS: U
SOURCE: Beta Analytics, Inc., 9600 Pennsylvania Avenue, Upper Marlboro, MD 20772, (301) 599-1570/1571
SUMMARY: Describes the multi-discipline hostile intelligence threat. Identifies the main adversaries and covers imagery intelligence (IMINT), signals intelligence (SIGINT), and human intelligence (HUMINT).

FRIEND AND FOE: THE NEW ESPIONAGE CHALLENGE

DATE: 1991 LENGTH: 20 min. MEDIUM: VC CLASS: U
SOURCE: Filmcomm, 641 North Avenue, Glendale Heights, IL 60139 (708) 790-3300
SUMMARY: Points out that despite the end of the Cold War, the foreign intelligence threat has not been eliminated, only altered. Identifies U.S. technology as a target for foreign intelligence collection and characterizes the government's role in support of industry to counter the threat.

HI-TECH TRAIL TO MOSCOW

DATE: 1983 LENGTH: 50 min. MEDIUM: VC CLASS: U
SOURCE: Films Incorporated, 5547 N. Ravenswood Avenue, Chicago, IL 60640-1199, (800) 323-4222, ext. 43
SUMMARY: BBC production examining the theft and sale to Moscow of advanced Western high technology. Common methods of operation and diversion routes through neutral countries are described.

INTERVIEWS WITH BOYCE, BELL, HELMICH AND LEE

DATE: LENGTH: 13 min. MEDIUM: VC, ID M56 1003 CLASS: U
SOURCE: National Security Agency (M56), Fort Meade, MD 20755-6000, (301) 688-6535
SUMMARY: A series of interviews with four individuals convicted of espionage, who describe how they were able to do it and explain their rationalization.

JONATHAN POLLARD-A PORTRAYAL

DATE: 1991 LENGTH: 18 min. MEDIUM: VC 1/2" 3/4" CLASS: U
SOURCE: FilmComm, 641 North Avenue, Glendale Heights, IL 60139, (708) 790-3300
SUMMARY: Reenacts the events at Naval Intelligence Command in Suitland, MD, that led to the realization Pollard was involved in more than just doing his job.

KGB CONNECTIONS: AN INVESTIGATION INTO SOVIET OPERATIONS IN NORTH AMERICA (2 TAPES)
DATE: 1980 LENGTH: 135 min. MEDIUM: VC 1/2" BETA CLASS: U
SOURCE: American Media, Box 4646, Westlake Village, CA 91359, (800) 282-2873
SUMMARY: Documentary examines the range of KGB operations in the U.S. from the theft of technological and industrial secrets to "disinformation" in the press; from penetration of the United Nations staff to covert support for extremist radical groups; from the infiltration of "illegals" to the recruitment at the highest levels of Government.

LEMON AID

DATE: LENGTH: 16 min. MEDIUM: VC, ID M56 1010 CLASS: U
SOURCE: National Security Agency (M56), Fort Meade, MD 20755-6000, (301) 688-6535
SUMMARY: Depicts the FBI's investigation of two Soviet employees of the United Nations Secretariat who were arrested for accepting classified information.

MILITARY AND THE NEWS MEDIA: A MATTER OF INTELLIGENCE

DATE: LENGTH: 60 min. MEDIUM: VC, ID M56 1011 CLASS: U
SOURCE: National Security Agency (M56), Fort Meade, MD 20755-6000, (301) 688-6535
SUMMARY: Explores the collision between the government's view of the national interest and the media's claims under the First Amendment.

OPERATION RED FOX

DATE: 1983 LENGTH: 27 min. MEDIUM: VC 3/4" 1/2", MP CLASS: U
SOURCE: DA: 501100, DF: 501100
SUMMARY: A docu-drama on the illegal acquisition of U.S. classified information and high technology by the Soviet KGB, through targeting of a Defense contractor and the supplier of sophisticated microelectronic production equipment.

THE PARTNERSHIP

DATE: 1989 LENGTH: 41 min. MEDIUM: VC 3/4" 1/2" CLASS: U
SOURCE: DA: 706124
SUMMARY: Uses current media examples of hostile intelligence service successes in recruiting civilians for espionage. Discusses how to protect yourself from a serious and determined threat, what to do if you are approached by an agent, and what to do if you suspect someone of spying.

THE SAFEGUARDING PROPRIETARY INFORMATION AUDIOVISUAL PROGRAM

DATE: 1985 LENGTH: 132 min. MEDIUM: VC 1/2" 3/4" ST CLASS: U
SOURCE: American Society for Industrial Security, 1655 North Fort Myer Drive, Suite 1200, Arlington, VA 22209-3198, (703) 522-5800
SUMMARY: An eleven-part series (12 min. each) that addresses all critical aspects of information protection, e.g., program and product development, computers, research, trade secrets, the electronic office, privacy, document management, industrial espionage.

SECURITY ORIENTATION FOR CLERICAL PERSONNEL

DATE: 1986 LENGTH: 25 min. MEDIUM: ST CLASS: U
SOURCE: DF: 604573
SUMMARY: Discusses proper handling procedures to follow when working with classified information. Explains how careless handling, lack of knowledge, or just plain innocent mistakes can lead to compromise of classified information. Target audience is USAF personnel.

SO EASY TO FORGET

DATE: LENGTH: 14 min. MEDIUM: VC, ID DAVIS 5006 CLASS: U
SOURCE: National Security Agency (M56), Fort Meade, MD 20755-6000, (301) 688-6535
SUMMARY: A foreign agent returning from his recent tour in the U.S. tells of common security discrepancies which occur in any office environment. He emphasizes how thoughtlessness and forgetfulness lead to security weaknesses.

SOMEONE IS WATCHING: PERSONAL SECURITY PRECAUTIONS

DATE: LENGTH: 15 min. MEDIUM: VC CLASS: U
SOURCE: Department of Energy/Argonne National Laboratory, 9700 S. Cass Avenue, Chicago, IL 60439-4828
SUMMARY: A former KGB intelligence officer discusses how hostile intelligence agencies target individuals with access to sensitive information.

SOMETHING OF VALUE

DATE: 1981 LENGTH: 10 min. MEDIUM: MP, VC CLASS: U
SOURCE: U.S. Security Authority for NATO Affairs, c/o ODUSD (SP), Room 3C277,
The Pentagon, Washington, DC 20301
SUMMARY: Animated tape portraying two groups of people. The first builds a
structure - something of value - in which its members can live in peace and
happiness. The second group, being suspicious, wants to destroy it.

SOVIET STRATEGIC PSYCHOLOGICAL OPERATIONS IN PEACETIME

DATE: 1988 LENGTH: 32 min. MEDIUM: VC 3/4" CLASS: U
SOURCE: DA: 701220
SUMMARY: Discusses the Soviet Unions campaign to influence world opinion against
the U.S. Soviet strategic psychological operations are defined as political,
military, economic, ideological and information activities aimed to create emotions,
attitudes or behavior favorable to the Soviet Union.

THE SOVIET THREAT

DATE: 1985 LENGTH: 30 min. MEDIUM: VC CLASS: U
SOURCE: Lockheed Missiles & Space Co., P.O. Box 3504, Attn: Security Training,
0/27-33 B509 Fac5, Sunnyvale, CA 94088-3504, (408) 742-4321
SUMMARY: Briefing on the hostile intelligence threat to U.S. Defense programs, with
the emphasis on the work of the Soviet KGB and GRU.

THE SPIES AMONG US

DATE: 1981 LENGTH: 52 min. MEDIUM: VC 1/2" 3/4" CLASS: U
SOURCE: Films Incorporated, 5547 N. Ravenswood Avenue, Chicago, IL 60640-1199,
(800) 323-4222, ext. 43
SUMMARY: NBC Special Report explores the extent and danger of Soviet bloc spy
activities in the U.S. Covers the range of Soviet intelligence gathering activities
including number and variety of agents involved, covert methods used and measures to
combat espionage by U.S. counterintelligence agencies.

STUDY IN BETRAYAL: MICHAEL WALKER

DATE: LENGTH: 18 min. MEDIUM: VC, ID M56 1040 CLASS: U
SOURCE: National Security Agency (M56), Fort Meade, MD 20755-6000, (301) 688-6535
SUMMARY: Convicted spy, Michael Walker, candidly discusses his espionage activities
against the U.S. intelligence community.

THE WAITING MAN

DATE: 1986 LENGTH: 45 min. MEDIUM: VC 3/4" 1/2" CLASS: U
SOURCE: DA: 802404
SUMMARY: "Lesson learned" type production based on the recruitment of a U.S.
enlisted man for the purpose of espionage by a hostile intelligence officer.

WILLIAM BELL: "A MODERN AMERICAN TRAGEDY"

DATE: 1982 LENGTH: 20 min. MEDIUM: VC CLASS: U
SOURCE: Films Incorporated, 5547 N. Ravenswood Avenue, Chicago, IL 60640-1199,
(800) 323-4222, ext. 43
SUMMARY: In "60 Minutes" interview Bell recounts his "bit-by-bit" enticement in
espionage by Polish intelligence operative Marian Zacharski and the sale of
classified technical information on advanced U.S. weapons systems.

YOU CAN MAKE A DIFFERENCE

DATE: 1993 LENGTH: 18 min. MEDIUM: VC 1/2" 3/4" CLASS: FOUO
SOURCE: FilmComm, 641 North Avenue, Glendale Heights, IL 60139, (708) 790-3300
SUMMARY: First in a series of six videos-each of which will focus on a different
aspect of espionage and what can be learned, from the point of view of the offender.

INFORMATION SECURITY**BURIED ALIVE**

DATE: LENGTH: 23 min. MEDIUM: VC 1/2" CLASS: U
SOURCE: Commonwealth Films, Inc., 223 Commonwealth Avenue, Boston, MA 02116,
(617) 262-5634
SUMMARY: Shows the importance of document retention and records management.

THE CONSTITUTION: THAT DELICATE BALANCE-NATIONAL SECURITY AND FREEDOM OF THE PRESS
DATE: 1984 LENGTH: 60 min. MEDIUM: VC 3/4" 1/2" CLASS: U
SOURCE: Intellimation, PO Box 1922, Santa Barbara, CA 93116, (800) 532-7637
SUMMARY: A provocative discussion of the requirements of national security vs. the rights of the press to collect and publish information regardless of classification or relationship to national defense.

THE ENHANCED INSPECTION

DATE: 1986 LENGTH: 17 min. MEDIUM: VC 1/2" 3/4" CLASS: U
SOURCE: American Society for Industrial Security, 1655 North Fort Myer Drive, Suite 1200, Arlington, VA 22209-3198, (703) 522-5800
SUMMARY: Panel discussion outlining the background and procedures of the new contractor facility inspection program.

HANDLING CLASSIFIED INFORMATION: BRIEFING FOR DEFENSE CONTRACTOR EMPLOYEES

DATE: 1984 LENGTH: 20 min. MEDIUM: ST CLASS: U
SOURCE: DF: 501103
SUMMARY: An overview of the practices and procedures for proper handling of classified material mandated by the Industrial Security Manual (DoD 5220.22-M).

INFORMATION SECURITY BRIEFING

DATE: 1987 LENGTH: 47 min. MEDIUM: VC, ST CLASS: U
SOURCE: Dub Centre, 10304 S. Dolfield Rd, Owings Mills, MD 21117, (800) 382-0080,
SUMMARY: Produced by Information Security Oversight Office (ISOO) and divided into three segments: (1) an overview of the information security system established under Executive Order 12356 (20 min.) (2) a detailed treatment of proper marking practices and procedures (15 min.) and; (3) highlights of the basic safeguarding requirements (12 min.).

THE INVISIBLE MAN

DATE: 1986 LENGTH: 12 min. MEDIUM: VC 1/2" 3/4" CLASS: U
SOURCE: American Society for Industrial Security, 1655 North Fort Myer Drive, Suite 1200, Arlington, VA 22209-3198, (703) 522-5800
SUMMARY: An introduction to private security and the roles played by security.

MARKING CLASSIFIED DOCUMENTS

DATE: 1986 LENGTH: 18 min. MEDIUM: ST CLASS: U
SOURCE: DF: 604572
SUMMARY: Provides initial instruction on how to mark classified documents. Target audience is USAF personnel.

MEMO FROM A GRATEFUL SPY

DATE: 1981 LENGTH: 10 min. MEDIUM: VC, MP CLASS: U
SOURCE: Coronet/MTI Film & Video, 108 Wilnot Road, Deerfield, IL 60015-5196, (800) 621-2131
SUMMARY: Compromise of classified information often results from a combination of employee negligence and careless security practices. Film is designed to increase awareness of this problem and motivate compliance with an organization's policy on information security.

PROTECTION OF PROPRIETARY INFORMATION: I SHOULDN'T BE TELLING YOU THIS, BUT...

DATE: 1980 LENGTH: 23 min. MEDIUM: VC, MP CLASS: U
SOURCE: Coronet/MTI Film & Video, 108 Wilnot Road, Deerfield, IL 60015-5196, (800) 621-2131
SUMMARY: Leaks of proprietary information lead a company to call in an outside investigator to catch "the spy." What he finds is carelessness, inattention and ignorance in security performance throughout the organization - rather than a single culprit. Includes slide and script program, brochures, posters and leaders guide.

SENSITIVE COMPARTMENTED INFORMATION AWARENESS BRIEFING

DATE: 1981 LENGTH: 29 min. MEDIUM: VC CLASS: FOUO
SOURCE: DA: 72035
SUMMARY: Explains extraordinary protection measures required for sensitive compartmented information (SCI) and stringent investigation prior to SCI access.

SECURITY EDUCATION

DATE: 1982 LENGTH: 20 min. MEDIUM: VC CLASS: U
SOURCE: DF: 504110
SUMMARY: Common security violations are acted out, followed by the correct procedure. Standard security regulations and guidelines are outlined.

THE SF 312

DATE: 1989 **LENGTH:** 13 min. **MEDIUM:** VC **CLASS:** U
SOURCE: Dub Centre, 10304 S. Dolfield Rd, Owings Mills, MD 21117, (800) 382-0080
SUMMARY: Information Security Oversight Office (ISOO) production on the Classified Nondisclosure Agreement. Answers most questions that cleared personnel will be asking concerning the SF 312 - reasons for signing, who must sign, what constitutes classified information, liabilities for not complying with its provision, etc.

SPACE FOR SECURITY

DATE: 1985 **LENGTH:** 29 min. **MEDIUM:** VC 3/4" **CLASS:** U
SOURCE: DF: 604008
SUMMARY: NASA production primarily dealing with mission security for the Space Transportation System. Discusses operations security, physical security, communications security and security of ADP systems, equipment and output.

THE SUPERVISOR'S ROLE IN SECURITY

DATE: 1987 **LENGTH:** 19 min. **MEDIUM:** MP, VC 3/4 1/2" BETA **CLASS:** U
SOURCE: Bureau of Business Practice, 24 Rope Ferry Road, Waterford, CT 06386, (800) 243-0876
SUMMARY: Shows supervisors techniques to ensure around-the-clock security. Dramatized sequences show where departments are vulnerable and what they can do about it.

FOREIGN TRAVEL

BRIEFING THE SUSCEPTIBLE TRAVELER

DATE: 1991 **LENGTH:** 12 min. **MEDIUM:** VC 1/2" **CLASS:** U
SOURCE: Pro Star International, P.O. Box 21526, Salt Lake City, UT 84121, (800) 775-0761
SUMMARY: A brief-the-briefer for security managers who need to brief employees traveling outside the U.S.

FOREIGN TRAVEL BRIEFING

DATE: 1981 **LENGTH:** 14 min. **MEDIUM:** ST **CLASS:** U
SOURCE: DF: 55003
SUMMARY: Briefing for those traveling to criteria countries. Outlines methods of entrapment used by hostile intelligence services and precautions against them. Scripts provided and keyed for manual slide advance.

FOREIGN TRAVEL BRIEFING - DON'T LEAVE HOME WITHOUT IT

DATE: 1991 **LENGTH:** 7 min. **MEDIUM:** VC 1/2" **CLASS:** U
SOURCE: Pro Star International, P.O. Box 21526, Salt Lake City, UT 84121, (800) 775-0761
SUMMARY: Designed for viewing by average employees traveling to a foreign country.

HOW TO TRAVEL ABROAD SAFELY

DATE: 1988 **LENGTH:** 30 min. **MEDIUM:** VC 1/2" **CLASS:** U
SOURCE: Coronet/MTI Film & Video, 108 Wilmot Road, Deerfield, IL 60015-5196, (800) 621-2131
SUMMARY: Discusses vehicle security, terrorism, travel tips, airport security, and hotel security.

REGIONAL TRAVEL BRIEFING - EUROPE

DATE: 1987 **LENGTH:** 38 min. **MEDIUM:** VC **CLASS:** U
SOURCE: DA: 706307
SUMMARY: Designed to reduce the probabilities of unpleasant experiences during travel, focusing on European countries. Explains why Americans are prime targets. Tells what Americans can do to accept European customs and to help Europeans except Americans.

REGIONAL TRAVEL BRIEFING - FAR EAST

DATE: 1987 **LENGTH:** 27 min. **MEDIUM:** VC **CLASS:** U
SOURCE: DA: 706308
SUMMARY: Points out how Americans may travel safely throughout countries of the Far East by observing local customs and remaining inconspicuous. Offers do's and don't's for Americans to keep a low profile and travel safely.

REGIONAL TRAVEL BRIEFING - LATIN AMERICA

DATE: 1987 LENGTH: 29 min. MEDIUM: VC

CLASS: U

SOURCE: DA: 706310

SUMMARY: Points out certain aspects of Latin America culture which could be sources of misunderstanding. Personal protective measures suggested. By varying routines and keeping a low profile, Americans can reduce vulnerability to attack.

REGIONAL TRAVEL BRIEFING - MIDDLE EAST

DATE: 1987 LENGTH: 26 min. MEDIUM: VC

CLASS: U

SOURCE: DA: 706309

SUMMARY: Helps American military members and government employees avoid attracting attention to themselves while in the Middle East. Provides information on the culture of this part of the world and symbolic prohibitions.

TERRORISM**BOMB THREAT**

DATE: 1986 LENGTH: 17 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: Coronet/MTI Film & Video, 108 Wilmot Road, Deerfield, IL 60015-5196, (800) 621-2131

SUMMARY: Discusses planning, searching, and evacuation techniques.

CHEMICAL AND BIOLOGICAL AGENT EFFECTS

DATE: 1991 LENGTH: 21 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 706133

SUMMARY: Presents a brief history of the use of chemical agents as early as the fifth century B.C. Also shows the effects of chemical and/or biological agents and how to counter these effects.

EVASIVE DRIVING...WHAT IF

DATE: 1988 LENGTH: 20 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 702048

SUMMARY: Illustrates the proper evasive techniques to be taken when encountering terrorist situations.

EXECUTIVE SAFETY & INTERNATIONAL TERRORISM: HOW TO TRAVEL ABROAD SAFELY

DATE: 1988 LENGTH: 24 min. MEDIUM: VC 3/4" 1/2" BETA

CLASS: U

SOURCE: Coronet/MTI Film & Video, 108 Wilmot Road, Deerfield, IL 60015-5196, (800) 621-2131

SUMMARY: Although business persons cannot control the environment in which they must travel, there are steps to take to avoid becoming the victim of an attack.

EXECUTIVE SAFETY & INTERNATIONAL TERRORISM: HOW TO PROTECT YOUR HOME

DATE: 1988 LENGTH: 30 min. MEDIUM: VC 3/4" 1/2" BETA

CLASS: U

SOURCE: Coronet/MTI Film & Video, 108 Wilmot Road, Deerfield, IL 60015-5196, (800) 621-2131

SUMMARY: A comprehensive security plan, with full participation from all members of the family, is the best way to deter a terrorist attack on your home. Although you can't control the actions of terrorists, you can take steps to make your home a high-risk target - one that potential attackers will avoid.

HARD TARGET

DATE: 1987 LENGTH: 16 min. MEDIUM: VC 3/4"

CLASS: U

SOURCE: DN: 803445

SUMMARY: Makes people aware of what terrorism is, what a terrorist does, how he does it, who he is and how to protect the command and the individual.

HOSTAGE/SITUATION MANAGEMENT

DATE: 1988 LENGTH: 21 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 702049

SUMMARY: Focuses on hostage taking, and how the hostage negotiation team operates. Discusses procedures to be followed when a terrorist attack occurs.

INSTALLATION TERRORISM COUNTERACTION PROGRAM

DATE: 1988 LENGTH: 19 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 702045

SUMMARY: This presentation discusses the Army's model for countering terrorism on military installations.

INTRODUCTION TO TERRORISM - PART I

DATE: 1990 LENGTH: 30 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 702280

SUMMARY: Defines terrorism and terrorist groups. Explains the objectives and the perspectives of terrorists. Also demonstrates proper and improper reactions to terrorist tactics and the tragic results when mistakes are made.

INTRODUCTION TO TERRORISM - PART II - TERRORIST OPERATIONS

DATE: 1990 LENGTH: 18 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 702281

SUMMARY: Reviews the basics phases of terrorist attacks. Demonstrates forms of attacks, defenses against attacks, negotiations, security, terrorist operations and tactics to avoid entrapment.

INTRODUCTION TO TERRORISM - PART III - SURVEILLANCE DETECTION

DATE: 1990 LENGTH: 19 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 702282

SUMMARY: Reviews and explains basic methods and characteristics of surveillance. Demonstrates tactics, combatants and methods of evasion used to detect terrorist surveillance.

INTRODUCTION TO TERRORISM - PART IV - HOSTAGE SURVIVAL

DATE: 1990 LENGTH: 22 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 702283

SUMMARY: Describes incidents, how to avoid terrorist traps and things to do to help build rapport with your captor. Demonstrates tactics and actions necessary to survive in a hostage situation.

INTRODUCTION TO TERRORISM, PART 1: HISTORY, PROFILES, PERSPECTIVES

DATE: 1986 LENGTH: 25 min. MEDIUM: VC

CLASS: U

SOURCE: Coronet/MTI Film & Video, 108 Wilmot Road, Deerfield, IL 60015-5196,
(800) 621-2131

SUMMARY: Provides an overview of terrorism and approaching threat. Identifies terrorist groups and discusses terrorism from different perspectives. Characteristics and ideology are discussed and organization of terrorist groups are explained.

INTRODUCTION TO TERRORISM, PART 2: TARGETS, ORGANIZATIONS, VIOLENCE

DATE: 1986 LENGTH: 28 min. MEDIUM: VC

CLASS: U

SOURCE: Coronet/MTI Film & Video, 108 Wilmot Road, Deerfield, IL 60015-5196,
(800) 621-2131

SUMMARY: Discusses the organization and training of terrorist groups. Portrays acts of violence, explores individual organizations - their internal structure, how they raise money, etc.

NO PLACE TO HIDE - THE STRATEGY AND TACTICS OF TERRORISM

DATE: 1985 LENGTH: 30 min. MEDIUM: VC 3/4"

CLASS: U

SOURCE: DA: 701633

SUMMARY: Explores the strategy and tactics of the international terrorist network. Suggests terrorist groups all follow a pattern which, if recognized gives the opportunity to anticipate the next development.

RESISTING TERRORIST INTERROGATION

DATE: 1989 LENGTH: 22 min. MEDIUM: VC 3/4"

CLASS: U

SOURCE: DA: 702034

SUMMARY: Demonstrates what a terrorist will do to make you lose your self esteem. Also techniques for resisting terrorist interrogation are shown and identifies and demonstrates the use of clandestine communication techniques which can be used by hostages when held by terrorist groups.

SAEDA AND TERRORISM

DATE: 1988 LENGTH: 26 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 702039

SUMMARY: Terrorists work systematically, they study routine security practices, and learn individuals' habits well in advance of a terrorist action. They target American forces for symbolic value, and individuals by means of bombings, assassinations, kidnappings, ambush and subversions. This docu-drama portrays a group of subversions carefully plotting the car bombing of a U.S. Army officer.

SELF-PROTECTIVE MEASURES AGAINST TERRORISTS

DATE: 1984 LENGTH: 25 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DN: 804720

SUMMARY: Points out ways to minimize chances for low risk personnel becoming a target for terrorists and presents precautionary measures that can be taken against military officers, civilians and State Department officials.

THE SENTRY IN TERRORISM COUNTERACTION

DATE: 1988 LENGTH: 16 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA702041

SUMMARY: Emphasizes the need for security conscious sentries who will minimize vulnerability to terrorist attack.

SHIPBOARD ANTITERRORIST SWIMMER DEFENSE

DATE: 1989 LENGTH: 15 min. MEDIUM: VC 3/4" 1/2" BETA II CLASS: C

SOURCE: DN: 804566

SUMMARY: Discusses anti-swimmer measures which may be take by U.S. ships in port or anchored where they are most accessible and vulnerable to terrorist attack.

SURVIVING HOSTAGE SITUATIONS

DATE: LENGTH: 27 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: Coronet/MTI Film & Video, 108 Wilmot Road, Deerfield, IL 60015-5196, (800) 621-2131

SUMMARY: Discusses and dramatizes real life scenarios on people dealing with terrorists and kidnappers.

SURVIVING TERRORIST KIDNAPPINGS

DATE: 1986 LENGTH: 15 min. MEDIUM: VC 3/4"

CLASS: FOUO

SOURCE: DA: 602007

SUMMARY: Points out several ways to avoid becoming a hostage of a terrorist group, and demonstrates how to survive a hostage situation.

TERRORISM - A PERSONAL THREAT

DATE: 1986 LENGTH: 17 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 604070

SUMMARY: Various members of the military describe their reactions to terrorist attacks on them personally.

TERRORISM - A REAL THREAT

DATE: 1986 LENGTH: 15 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DN: 604069

SUMMARY: Points out the real threat of terrorism to men and women of the U.S. military on overseas assignments. Cites examples of terrorist attacks which were planned to receive maximum media coverage.

TERRORISM - A SURVIVABLE THREAT

DATE: 1986 LENGTH: 19 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 604078

SUMMARY: Hazards of foreign assignments are pointed out. Shows examples of military members who became careless and lost their lives at the hands of terrorists.

TERRORISM AWARENESS

DATE: 1988 LENGTH: 31 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DN: 702040

SUMMARY: The prevention of terrorism begins with awareness. Awareness means developing a security mindset: Act the way you would in a high-crime neighborhood and don't leave sensitive documents exposed.

TERRORISM CRISIS MANAGEMENT

DATE: 1988 LENGTH: 17 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DN: 702050

SUMMARY: Demonstrates and explains procedures to be followed when a terrorist act occurs on an Army installation.

TERRORISM INCIDENT ANALYSIS PARTS I-V

DATE: 1988 LENGTH: 128 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 702037

SUMMARY: Bombing, ambush and assassination, kidnapping, skyjacking and hostage/barricade are terrorism incidents analyzed in this five part program.

TERRORISM: WAR IN THE SHADOWS**DATE:** 1986 **LENGTH:** 48 min. **MEDIUM:** VC 3/4"**CLASS:** U**SOURCE:** Arthur Mokin Productions, Inc., P.O. Box 1866, Santa Rosa, CA 95402, (707) 542-4868**SUMMARY:** CBS reports program focuses on the unconventional war being waged by terrorists in many countries of the world. Includes scenes following attacks on embassies, assassination, bombings and hijackings.

TERRORIST BOMB AWARENESS**DATE:** 1989 **LENGTH:** 21 min. **MEDIUM:** VC 3/4"**CLASS:** U**SOURCE:** DA: 702051**SUMMARY:** Reviews suggested procedures for dealing and handling a terroristic bomb threat. Shows different types of Improvised Explosive Devices used by terrorist, how to plan for bomb threats, reaction to bomb incidents and bomb search techniques.

TERRORIST SMALL BOAT ATTACK ON MOORED U.S. NAVY SHIPS**DATE:** 1989 **LENGTH:** 23 min. **MEDIUM:** VC 3/4" 1/2 BETA II**CLASS:** C**SOURCE:** DN: 804567**SUMMARY:** Provides background information on terrorist threats; examines terrorist small boat attacks and makes recommendations for ship defense.

TIME OF THE JACKALS**DATE:** 1986 **LENGTH:** 50 min. **MEDIUM:** VC 3/4"**CLASS:** U**SOURCE:** Films Incorporated, 5547 N. Ravenswood Avenue, Chicago, IL 60640-1199, (800) 323-4222, ext. 43**SUMMARY:** Deals with transnational terrorism, focusing on the activities of on Ilich Ramirez Sanchez (Carlos of the Jackals). Presents a re-creation of the firebombing attack in Paris in 1973. Provides a background of Carlos's terrorist training and alleged political affiliations.

TRENDS IN TERRORISM**DATE:** 1988 **LENGTH:** 30 min. **MEDIUM:** VC 3/4" 1/2"**CLASS:** U**SOURCE:** DA: 702038**SUMMARY:** Highlights basic tactics used by terrorists in Europe and in the U.S. The tactics, targets and technology used by terrorists have been changing because of counteraction activities.

LAW ENFORCEMENT**COME-ALONG, THE****DATE:** 1980 **LENGTH:** 31 min. **MEDIUM:** VC 3/4" 1/2"**CLASS:** U**SOURCE:** DA: 30515**SUMMARY:** Demonstrates several different come-alongs (techniques of unarmed defense) by military police in the apprehension of offenders from the passive to the violent.

INTELLIGENCE OVERSIGHT**DATE:** 1990 **LENGTH:** 28 min. **MEDIUM:** VC 1/2"**CLASS:** U**SOURCE:** DN: 804640**SUMMARY:** Intelligence Oversight (legal regulations of intelligence activities) and its functions. Explains the statutory and constitutional provision that impose personal responsibility and liability on all military and civilian personnel. Also provides guidelines for collection, retention and dissemination of intelligence information.

INTOXICATED DRIVER (DETECTION AND TESTING)**DATE:** 1986 **LENGTH:** 18 min. **MEDIUM:** VC 3/4" 1/2"**CLASS:** U**SOURCE:** DA: 706019**SUMMARY:** Gives statistics on accidents, many fatal, involving the use of alcohol. Military police detection methods recommended to deter violations include regular trained patrols, systematic gate inspections, or a cone maze. Gives some obvious clues to look for and demonstrates sobriety tests used to establish probable cause.

MILITARY POLICE WITNESS IN COURT**DATE:** 1982 **LENGTH:** 38 min. **MEDIUM:** VC 3/4" 1/2"**CLASS:** U**SOURCE:** DA: 30521**SUMMARY:** Illustrates the importance of Military Police to testify in a calm and confident manner when appearing as a witness in court.

PROTECTIVE SERVICE TECHNIQUES - PARTS I - V

DATE: 1988 LENGTH: 68 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 702044

SUMMARY: PART I: Missions, roles, and responsibilities of protective service (15 min.). PART II: Planning considerations for protective service missions (17 min.). PART III: Equipping and training for protective service (13 min.). PART IV: Capabilities and limitations of protective service (11 min.). PART V: Protective service management (12 min.).

SPECIAL REACTION TEAM TECHNIQUES - PARTS I - V

DATE: 1988 LENGTH: 79 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 702043

SUMMARY: Addresses the threat of a growing number of terrorist and criminal attacks and how to deal with them through Special Reaction Team (SRT) techniques. PART I: Pre-planning phase. PART II: Immediate action phase. PART III: Execution planning phase. PART IV: The execution phase. PART V: Post execution phase.

TECHNIQUES OF CRIME SCENE PROCESSING - PARTS I AND II

DATE: 1990 LENGTH: 53 min. MEDIUM: VC 3/4" 1/2"

CLASS: U

SOURCE: DA: 706163 (Part I), DA: 707541 (Part II)

SUMMARY: Focuses on processing the crime scene; documenting, photographing, measuring, sketching and protecting the crime scene. Shows how to record the data.

VEHICLE BOMB SEARCH PROCEDURES

DATE: 1990 LENGTH: 12 min MEDIUM: VC 3/4"

CLASS: U

SOURCE: DN: 112961

SUMMARY: Explains and demonstrates some of the methods of planting car bombs, specific methods of car bomb search to include sedan and tactical vehicles, and how to spot tampering. Explains proper procedures to follow if a car bomb is found.

CRIME PREVENTION

ARE YOU SAFE?

DATE: LENGTH: 47 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: National Crime Prevention Council, 1700 K. Street NW, 2nd Floor, Room 3817, Washington, DC 20006, (202) 466-6272

SUMMARY: Reviews questions and answers on crime prevention. Dramatizes real life scenarios and provides security and safety precautions; handouts are provided.

BANK ROBBERY

DATE: LENGTH: 12 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: Coronet/MTI Film & Video, 108 Wilmet Road, Deerfield, IL 60015-5196, (800) 621-2131

SUMMARY: Discusses planning and preventing techniques.

DATE ACQUAINTANCE RAPE

DATE: 1987 LENGTH: 15 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: NCIS

SUMMARY: Gives statistical data, frequency and percentage of rapes where the subject is known to the victim. How to avoid placing oneself in a position of vulnerability.

THE DOMESTIC DILEMMA

DATE: 1987 LENGTH: 15 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: NCIS

SUMMARY: Overview of spousal abuse. How and where to seek help and how to control your domestic environment.

DRUG ABUSE PREVENTION KIT

DATE: 1988 LENGTH: 15 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: NCIS

SUMMARY: Drug abuse prevention kit for presentation to dependent children, ages 5 - 12 years. McGruff teaches children how to "Say No" to drugs. Kit has audio cassette, coloring sheets and instructor guide.

HANDGUN SAFETY

DATE: 1987 LENGTH: 15 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: NCIS

SUMMARY: Graphically depicts, in two scenarios, the proper methods for storing handguns and ammunition in the home.

THE ICE AGE

DATE: 1988 LENGTH: 10 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: NCIS

SUMMARY: Introduction to "ICE" a new methamphetamine which is threatening to hit the market in the U.S. Describes where it is manufactured, how it is routed, affect on the body, paraphenalia associated with use and shows actual crystals of "ICE".

IT STARTS WITH YOU

DATE: 1987 LENGTH: 37 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: Coronet/MTI Film & Video, 108 Wilmot Road, Deerfield, IL 60015,
(800) 621-2131

SUMMARY: Discusses security in the office, personal security and professional integrity in safeguarding information from outsiders or competitors; handouts are provided.

LIVING IT DOWN

DATE: LENGTH: 16 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: Coronet/MTI Film & Video, 108 Wilmot Road, Deerfield, IL 60015,
(800) 621-2131

SUMMARY: Reviews the consequences of stealing/shoplifting.

NO SECOND CHANCE

DATE: 1988 LENGTH: 10 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: NCIS

SUMMARY: Effectively depicts DWI/DUI related accidents and the impact on families.

ON THE LOOKOUT

DATE: 1986 LENGTH: 15 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: NCIS

SUMMARY: Neighborhood crime including confidence games and precautions taken to avoid being swindled.

PROTECT YOUR HOME

DATE: 1986 LENGTH: 30 min. MEDIUM: ST

CLASS: U

SOURCE: NCIS

SUMMARY: Produced by KWIKSET, regards locks and locking devices for home security. Recommends lock types and installation hardware for maximizing entry security.

RAPE: AN ACT OF VIOLENCE

DATE: 1987 LENGTH: 15 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: NCIS

SUMMARY: Information on reporting rapes, including frequency of occurrence, vulnerability study, prevention methods for women, responses to attack, and how to "read" the subject.

SAFETY NET

DATE: 1987 LENGTH: 15 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: NCIS

SUMMARY: Adapted from a slide presentation, program deals with symptoms of child abuse, how to report suspected cases and intervention methods.

OPERATIONS SECURITY**BUILDING BETTER BARRIERS: THE OPSEC ASSESSMENT PROCESS**

DATE: LENGTH: 13 min. MEDIUM: VC

CLASS: U

SOURCE: Department of Energy/Argonne National Laboratory, 9700 S. Cass Avenue,
Chicago, IL 60439-4828

SUMMARY: How OPSEC assessments can assist program managers and OPSEC planners in identifying vulnerabilities and proposing countermeasures to prevent adversaries from collecting critical information.

INTELLIGENCE THREAT TO OPERATIONS SECURITY

DATE: 1987 LENGTH: 26 min. MEDIUM: ST

CLASS: U

SOURCE: DF: 607018

SUMMARY: Intended to provide unit OPSEC officers with understanding of threat to the USAF posed by hostile intelligence agencies.

MAGNETS IN THE HAYSTACK

DATE: LENGTH: 12 min. MEDIUM: VC

CLASS: U

SOURCE: Department of Energy/Argonne National Laboratory, 9700 S. Cass Avenue, Chicago, IL 60439-4828

SUMMARY: Likens sensitive information to needles in a haystack, how an adversary is constantly looking for "magnets" to get at this information, and how OPSEC can provide countermeasures.

OPERATIONS SECURITY

DATE: LENGTH: 22 min. MEDIUM: VC 1/2"

CLASS: S

SOURCE: Defense Nuclear Agency

SUMMARY: Concentrates on indicators of critical information. Begins with examples on the football field and then applies concepts to U.S. Pacific Command.

OPSEC AND COUNTERNARCOTICS: WHO'S WATCHING WHO?

DATE: 1993 LENGTH: 17 min. MEDIUM: VC 1/2"

CLASS: U

SOURCE: Interagency OPSEC Support Staff, 6411 Ivy Lane, Suite 400, Greenbelt, MD 20770-1405, (301) 982-0323

SUMMARY: Lessons learned about OPSEC are shared by those involved in the drug war. Experiences shared encompass a spectrum from the street cop to senior DoD personnel. The USCG is a contributor.

THE OPSEC PICTURE PUZZLE

DATE: LENGTH: 13 min. MEDIUM: VC

CLASS: U

SOURCE: Department of Energy/Nevada Operations Office, OPSEC Program Manager, P.O. Box 98518, Las Vegas, NV 89193

SUMMARY: Demonstrates how individuals can unintentionally aid an adversary in building a "picture puzzle," and how OPSEC can deny an adversary this information.

OPSEC: PROTECTING OUR EDGE

DATE: 1992 LENGTH: 9 min. MEDIUM: VC

CLASS: U

SOURCE: Interagency OPSEC Support Staff, 6411 Ivy Lane, Suite 400, Greenbelt, MD 20770-1405, (301) 982-0323.

SUMMARY: The importance of OPSEC in protecting sensitive technological and economic information from loss to foreign competitors.

OPSEC TRAINING AT PATUXENT RIVER NAVAL TEST CENTER

DATE: LENGTH: 29 min. MEDIUM: VC

CLASS: U

SOURCE: Flight Test & Engineering Group, Code CT33, Naval Air Warfare Center, Patuxent River, MD 20670, (301) 826-1139

SUMMARY: How OPSEC can protect programs and test activities at the Center.

COMPUTER SECURITY**BILLION DOLLAR BUBBLE**

DATE: 1981 LENGTH: 60 min. MEDIUM: VC

CLASS: U

SOURCE: Films Incorporated, 5547 N. Ravenswood Avenue, Chicago, IL 60640-1199, (800) 323-4222, ext. 43

SUMMARY: BBC report on the major computer fraud case involving Equity Funding Corporation, Los Angeles, CA

COMPUTER REMOTE TERMINAL SECURITY

DATE: 1983 LENGTH: 10 min. MEDIUM: VC 3/4"

CLASS: U

SOURCE: DF: 601741

SUMMARY: Explains one way of implementing computer remote terminal security.

COMPUTER SECURITY

DATE: 1985 LENGTH: 24 min. MEDIUM: VC

CLASS: U

SOURCE: Coronet/MTI Film & Video, 108 Wilnot Road, Deerfield, IL 60015, (800) 621-2131

SUMMARY: Points out that those who work with computer systems have an obligation to preserve the integrity of the information that is stored. Gives guidelines for formulating and implementing a computer security strategy.

COMPUTER SECURITY AWARENESS**DATE:** 1985 **LENGTH:** 6 min. **MEDIUM:** ST**CLASS:** U**SOURCE:** U.S. Department of Agriculture, Photography Division, Office of Governmental & Public Affairs, Room 4404, South Building, Washington, DC 20250-1300**SUMMARY:** Basic orientation for new users of network computer systems. Motivational and educational on basic principles for users, e.g., password control.

COMPUTER SECURITY: MAKE THE COMMITMENT**DATE:** 1989 **LENGTH:** 15 min. **MEDIUM:** VC**CLASS:** U**SOURCE:** DA: 708556**SUMMARY:** Illustrates computer security practices by presenting realistic computer security problems and situations, and what happens when computer security is not maintained. Discusses responsibilities and the importance of protecting equipment, area, passwords, files and unattended terminals.

COMPUTER SYSTEM SECURITY: ACCESS CONTROL**DATE:** 1985 **LENGTH:** 16 min. **MEDIUM:** VC**CLASS:** U**SOURCE:** National Computer Security Center, Attn: S33, 9800 Savage Road, Ft. Meade, MD 20755-6000**SUMMARY:** Discusses motivations for computer crime. Talks about the use of "distrust" to prevent tampering and computer crime - distrust of physical security systems, communication systems, and operational procedures.

COMPUTER SYSTEM SECURITY: ACCESS-THE IN'S AND OUT'S**DATE:** 1985 **LENGTH:** 20 min. **MEDIUM:** VC**CLASS:** U**SOURCE:** National Computer Security Center, Attn: S33, 9800 Savage Road, Ft. Meade, MD 20755-6000**SUMMARY:** Focuses on the importance of a trusted computer system and the components of such a system including physical security, communications security and personnel security. Discusses tricks and techniques used in computer crime and some of the motivators behind such crime.

COMPUTER VIRUS DEFENSE: PREVENTION, DETECTION, CURE**DATE:** 1992 **LENGTH:** 20 min. **MEDIUM:** VC**CLASS:** U**SOURCE:** Commonwealth Films, Inc., 223 Commonwealth Avenue, Boston, MA 02116, (617) 262-5634**SUMMARY:** Includes how to safeguard against entry of malicious code by controlling access through passwords; how to recognize the presence of a virus before it infects a network; how to get rid of a virus; how to protect against reinfection, etc.

CORPORATE COMPUTER SECURITY STRATEGY - STRATEGIES**DATE:** 1984 **LENGTH:** 45 min. **MEDIUM:** VC**CLASS:** U**SOURCE:** National Education Training Group, 1751 W. Diehl Road, Napierville, IL 60563, (708) 369-3000**SUMMARY:** Identifies examples of management security objectives and procedures for selecting and designing security controls.

CORPORATE COMPUTER SECURITY STRATEGY - TECHNIQUES**DATE:** 1984 **LENGTH:** 45 min. **MEDIUM:** VC**CLASS:** U**SOURCE:** National Education Training Group, 1751 W. Diehl Road, Napierville, IL 60563, (708) 369-3000**SUMMARY:** Provides basic introduction to corporate computer security. Specifically focuses on the basic security controls that can be applied to computer systems.

CORPORATE COMPUTER SECURITY STRATEGY - THREATS**DATE:** 1984 **LENGTH:** 45 min. **MEDIUM:** VC**CLASS:** U**SOURCE:** National Education Training Group, 1751 W. Diehl Road, Napierville, IL 60563, (708) 369-3000**SUMMARY:** Describes the consequences of inadequate security and accuracy controls in corporate computer security. Recognizes threats most likely to strike the corporation and identifies the potential damage caused by different types of computer threat.

DATA SECURITY: BE AWARE OR BEWARE**DATE:** 1984 **LENGTH:** 20 min. **MEDIUM:** VC**CLASS:** U**SOURCE:** Commonwealth Films, Inc., 223 Commonwealth Avenue, Boston, MA 02116, (617) 262-5634**SUMMARY:** A series of vignettes dramatizes some common but serious breaches of computer security. Show the consequences and illustrates correct procedures.

ELECTRONIC DELINQUENTS

DATE: 1983 LENGTH: 14 min. MEDIUM: VC, MP CLASS: U
SOURCE: Coronet/MTI Film & Video, 108 Wilmot Road, Deerfield, IL 60015-5196,
(800) 621-2131
SUMMARY: ABC "20/20" segment explains how unauthorized users gain access to a computer system and the losses in time, money and information which can result.

INFORMATION SYSTEMS - SECURITY IS THE PASSWORD

DATE: 1985 LENGTH: 16 min. MEDIUM: MP, VC 1/2" 3/4" CLASS: U
SOURCE: DF: 603157
SUMMARY: Acquaints non-computer personnel with the major component parts of the ADP security by demonstrating how it relates to the ASAF mission. Target audience is all ranks, grades and skill levels who use or will be working with computers.

INVASION OF THE DATA SNATCHERS

DATE: 1989 LENGTH: 20 min. MEDIUM: VC CLASS: U
SOURCE: Commonwealth Films, Inc., 223 Commonwealth Avenue, Boston, MA 02116,
(617) 262-5634
SUMMARY: Blends information, practical tips, fact-based incidents and action entertainment-dramatized in detective-comics style.

THE KGB, THE COMPUTER AND ME

DATE: 1990 LENGTH: 58 min. MEDIUM: VC 1/2" 3/4" CLASS: U
SOURCE: Coronet/MTI Film & Video, 108 Wilmot Road, Deerfield, IL 60015-5196,
(800) 621-2131
SUMMARY: Tells the story of international computer espionage: Clifford Stoll, a computer systems manager, discovers that a hacker has gained access to the lab's computers and is perusing supposedly secret files. The data Stoll collects links the hacker to a West German spy ring that is selling sensitive information from U.S. military computers to the KGB.

LOCKING THE DOOR

DATE: 1987 LENGTH: 20 min. MEDIUM: VC CLASS: U
SOURCE: Commonwealth Films, Inc., 223 Commonwealth Avenue, Boston, MA 02116,
(617) 262-5634
SUMMARY: Dramatizes six common breaches of computer security: external disclosures of secrets; inhouse leaks of confidential files; unauthorized alteration of stored data; damage and loss of data; illegal copying; and theft.

LOCKOUT! INFORMATION SECURITY AND DATA CLASSIFICATION

DATE: 1990 LENGTH: 22 min. MEDIUM: VC CLASS: U
SOURCE: Commonwealth Films, Inc., 223 Commonwealth Avenue, Boston, MA 02116,
(617) 262-5634
SUMMARY: This video's television game show reviews and tests the viewer's knowledge about methods of classifying, labeling and protecting data and hardware.

MAXIMUM SECURITY: MICROCOMPUTER DATA & HARDWARE SECURITY

DATE: 1990 LENGTH: 15 min. MEDIUM: VC CLASS: U
SOURCE: Commonwealth Films, Inc., 223 Commonwealth Avenue, Boston, MA 02116,
(617) 262-5634
SUMMARY: Topics include password protection, classifying data by levels of security and protection, storage, equipment protection, user-written program testing, risks of running untested software and defending against data loss.

MUM'S THE WORD: PC AND LAN DATA SECURITY

DATE: 1990 LENGTH: 20 min. MEDIUM: VC CLASS: U
SOURCE: Commonwealth Films, Inc., 223 Commonwealth Avenue, Boston, MA 02116,
(617) 262-5634
SUMMARY: Vignettes illustrate the vulnerability of PCs and LANs, back-up procedures, data recovery, physical hazards, diskette security/storage/handling, password selection/protection/secretcy, computer viruses, unauthorized access, bootlegged/untested software, bulletin board software, etc.

SPIES IN THE WIRES

DATE: 1983 LENGTH: 48 min. MEDIUM: VC CLASS: U
SOURCE: Films Incorporated, 5547 N. Ravenswood Avenue, Chicago, IL 60640-1199,
(800) 323-4222, ext. 43
SUMMARY: BBC production examines the vulnerability of computer systems to tampering and data interception.

TIME BOMB

DATE: 1981 LENGTH: 35 min. MEDIUM: MP VC 3/4" 1/2" BETA 1 CLASS: U
SOURCE: Visucom Productions, Box 5472, Redwood City, CA 94063, (415) 364-5566
SUMMARY: Tells the story of a computer department overtaken by a series of disasters. Details a story of security failures which threaten the installation and data program.

UNDER WRAPS: INFORMATION SECURITY

DATE: 1990 LENGTH: 19 min. MEDIUM: VC CLASS: U
SOURCE: Commonwealth Films, Inc., 223 Commonwealth Avenue, Boston, MA 02116, (617) 262-5634
SUMMARY: Dramatized scenes show how almost every kind of written, verbal, computer, and other forms of corporate information and data - even that which may seem trivial, routine, or incomprehensible to outsiders - is vulnerable and can be extremely valuable in the wrong hands.

WE LOST CONTROL: ILLEGAL SOFTWARE DUPLICATION

DATE: 1992 LENGTH: 16 min. MEDIUM: VC CLASS: U
SOURCE: Commonwealth Films, Inc., 223 Commonwealth Avenue, Boston, MA 02116, (617) 262-5634
SUMMARY: Dramatizes one company's software crisis. As the company learns, ignorance is no excuse under the Copyright Protection Act. Designed to show what employees can do to protect their organization and themselves from non-compliance.

COMMUNICATIONS SECURITY**COMMUNICATIONS SECURITY BRIEFING**

DATE: 1983 LENGTH: 18 min. MEDIUM: ST CLASS: U
SOURCE: DF: 600295
SUMMARY: An introductory message for incoming personnel centering around do's and don'ts relating to communications security.

CONFIDENTIALLY SPEAKING

DATE: 1980 LENGTH: 14 min. MEDIUM: MP, VC CLASS: U
SOURCE: GTE Service Corporation, Attn: AV Librarian, 1 Stamford Forum, Stamford, CT 06904, (203) 965-2289
SUMMARY: Focuses upon the dangers of discussing any sensitive information over the telephone and other telecommunications vulnerabilities.

COUNTER THE THREAT WITH PROTECTIVE TECHNOLOGIES

DATE: LENGTH: 16 min. MEDIUM: VC 1/2" CLASS: FOUO
SOURCE: National Security Agency (M56), Fort Meade, MD 20755-6000, (301) 688-6535
SUMMARY: Discusses human intelligence threats; protecting information; espionage; alerts COMSEC custodians of possible compromises; checks for tampering with canisters, seals, bags, tape, breaking of screws, etc.

THE GIVEAWAY - COMMUNICATIONS SECURITY

DATE: 1985 LENGTH: 25 min. MEDIUM: MP, VC 1/2" 3/4" CLASS: FOUO
SOURCE: DF: 602312
SUMMARY: Tells the story of three incidents where people sold sensitive material to foreign powers; how they were detected and arrested. Stresses the ways in which people engaged in such activities may be recognized by their co-workers.

INTO THIN AIR

DATE: 1989 LENGTH: 48 min. MEDIUM: VC CLASS: U
SOURCE: Information Security Inc., Dept V, 1001 Spring Street, Suite 123, Silver Spring, MD 20910, (301) 565-8168
SUMMARY: Dramatizes the threats and vulnerabilities which government organizations, industry and individuals face in using unprotected communications in their day-to-day operations. Depicts how easily sensitive information can be obtained by intercepting satellite, microwave and cellular radio transmissions with commercially available equipment.

SECURITY BRIEFING (COMSEC/OPSEC)

DATE: 1981 LENGTH: 8 min. MEDIUM: ST CLASS: U
SOURCE: DN: 53077
SUMMARY: Explains communications security and operations security, including crypto, emission, transmission and physical security.

WAS IT SOMETHING I SAID?

DATE: 1985 **LENGTH:** 13 min. **MEDIUM:** MP, VC

CLASS: U

SOURCE: Coronet/MTI Film & Video, 108 Wilmot Road, Deerfield, IL 60015-5196,
(800) 621-2131

SUMMARY: Illustrates that employees at all levels are responsible for proprietary, or classified information. A telecommunications company is about to embark on a satellite project when loose talk, gossip and carelessness put the project in jeopardy.

MISCELLANEOUS

PROFESSIONAL SECURITY TRAINING NETWORK (PSTN)

1303 MARSH LANE

CARROLLTON, TX 75006

(800) 942-7786

This television program is delivered monthly to subscribers on videotapes. It provides current and vital security-related news, information and training for the security professional. PSTN provides programming for every member of the security department, from security decision-makers to line security officers. It covers a wide range of topics for security officers, security supervisors and specialists, and security directors/managers.

It also includes a twelve part Basic Security Training Officer series, complete with instructor guides, student handouts, and test materials. The module program consists of:

- Introduction to Security
- Importance of the Security Officer
- Legal Issues - Part I
- Legal Issues - Part II
- Human & Public Relations
- Communications
- Patrol
- General Duties
- Report Writing
- Fire Prevention & Control
- Emergency Situations
- Safety

EXHIBIT 2-4

LITERATURE

Listed below is a compilation of literature books which are available from libraries, bookstores and publishers; it is not a complete list. The Coast Guard has not evaluated each source/product and makes no endorsement as to quality or suitability.

Each entry begins with the author (in alphabetical order under each subject heading), then title (underlined), publisher and date of publication.

GENERAL

- Berger, David L. Industrial Security. Butterworth-Heinemann, 1979.
- Carson, Charles R. Managing Employee Honesty. Butterworth-Heinemann, 1977.
- Cherry, Don T. Total Facility Control. Butterworth-Heinemann, 1986.
- Coleman, John L. The Security Supervisor's Handbook: A Guide for the Private Security Primary Manager. Charles C. Thomas Publishers, 1987.
- Colling, Russell. Hospital Security. (3rd ed.) Butterworth-Heinemann, 1992.
- Coster, Anthony. Security in Commerce & Industry. Butterworth-Heinemann 1988.
- Fennelly, Lawrence. Museum, Archive, and Library Security. Butterworth-Heinemann, 1983.
- Hertig, Christopher A. & Bittner, Gary E. Report Writing for Security Personnel. Butterworth-Heinemann, 1991.
- Higgins, Clay. Applied Security Management. Charles C. Thomas Publishers 1990.
- Inbau, Fred, Aspen, Marvin & Spiotto, James. Protective Security Law. Butterworth-Heinemann, 1983.
- International Foundation for Protection Officers. The Protection Officer Training Manual. (5th ed.), Butterworth-Heinemann, 1992.
- Luis, Ed S. Office & Office Building Security. Butterworth-Heinemann, 1973.
- Lyons, Stanley L. Security of Premises Manual for Managers. Butterworth-Heinemann, 1988.
- Neill, W. Modern Retail Risk Management. Butterworth-Heinemann, 1981.
- Post, Richard S. & Schachtsiek, David A. Security Manager's Desk Reference. Butterworth-Heinemann, 1986.
- Purpura, Philip P. Modern Security & Loss Prevention Management. Butterworth-Heinemann, 1989.
- Sennewald, Charles A. Security Consulting. Butterworth-Heinemann, 1989.
- Siljander, Raymond P. Introduction to Business and Industrial Security and Loss Control: A Primer for Public Law Enforcement and Private Security Personnel. Charles C. Thomas Publishers, 1991.
- Underwood, Grahame. The Security of Buildings. Butterworth-Heinemann, 1984.
- Wagner, Thomas J, Wingert, Emily A. & Wanat, John A. Basic Security Training Manual. Charles C. Thomas Publishers, 1979.
- Wanat, John, Guy, Edward & Merrigan, Jr, John. Supervisory Techniques for the Security Professional. Butterworth-Heinemann, 1981.
- Westhuizen, J. V. Security Management. Butterworth-Heinemann, 1991.

PHYSICAL SECURITY

- Barnard, Robert L. Intrusion Detection Systems (2nd ed.). Butterworth-Heinemann, 1988.
- Berger, David. Security for Small Businesses. Butterworth-Heinemann, 1981.
- Bottom, Norman R. & Kostanoski, John. Security and Loss Control. MacMillan Publishing Company, Inc., 1983.
- Bowers, Dan M. Access Control and Personal Identification Systems. Butterworth-Heinemann, 1988.
- Broder, James F. Risk Analysis & Security Survey. Butterworth-Heinemann 1984.
- Capel, Vivian. Security Systems & Intruder Alarms. Butterworth-Heinemann 1989.
- Cassidy, Kevin A. Fire Safety & Loss Prevention. Butterworth-Heinemann 1992.
- Cleary, James Jr. Prosecuting the Shoplifter: A Loss Prevention Strategy. Butterworth-Heinemann, 1986.
- Cumming, Neil. Security, A Guide to Security System Design and Equipment Selection and Installation (2nd ed.). Butterworth-Heinemann, 1992.
- Eisenstat, Norman C. The Science of Selling Alarm Systems. Butterworth-Heinemann, 1984.
- Fay, John J. Drug Testing. Butterworth-Heinemann, 1990.
- Fennelly, Lawrence J. Effective Physical Security. Butterworth-Heinemann 1992.
- Gallery, Shari. Current Issues in Security Management. Butterworth-Heinemann, 1988.
- Gigliotti, Richmond & Jason, Ronald C. Emergency Planning for Maximum Protection. Butterworth-Heinemann, 1991.
- Green, Gion. Introduction to Security. (5th ed.) Butterworth-Heinemann, 1992.
- Hayes, Read. Retail Security & Loss Prevention. Butterworth-Heinemann, 1991.
- Jones, Lawrence S. Cargo Security: A Nuts and Bolts Approach. Butterworth-Heinemann, 1983.
- Jones, Peter H. Retail Loss Control. Butterworth-Heinemann, 1990.
- Knowles, Graham. Bomb Security Guide. Butterworth-Heinemann, 1976.
- Kyle, Thomas G. & Aldridge, James. Security Closed Circuit Television Handbook: Applications & Technical. Charles C. Thomas Publishers, 1992.
- McTague, Dan & Smith, Doug. The Alarm Book. Butterworth-Heinemann, 1987.
- Moore, Kenneth C. Airport, Aircraft and Airline Security. (2nd ed.) Butterworth-Heinemann, 1991.
- National Crime Prevention Institute. The Use of Locks in Physical Crime Prevention. Butterworth-Heinemann, 1987.
- National Crime Prevention Institute & D'Addario, Francis J. Loss Prevention Through Crime Analysis. Butterworth-Heinemann, 1989.
- Neidle, Michael. Emergency and Security Lighting Handbook. Butterworth-Heinemann, 1988.
- Post, Richard S. & Kingsberry, Arthur A. Security Administration: An Introduction. (4th ed.) Charles C. Thomas Publishers, 1991.
- Purpura, Phillip. Security and Loss Prevention. (2nd ed.) Butterworth-Heinemann, 1991.

- Sanger, John. Basic Alarm Electronics. Butterworth-Heinemann, 1988.
- Sanger, John. The Alarm Dealer's Guide. Butterworth-Heinemann, 1985.
- Sanger, John. More Kinks & Hints. Butterworth-Heinemann, 1986.
- Schnabolk, Charles. Physical Security, Practices and Technology. Butterworth-Heinemann, 1983.
- Schum, John L. Electronic Locking Devices. Butterworth-Heinemann, 1988.
- Sennewald, Charles. Effective Security Management. (2nd ed.) Butterworth-Heinemann, 1985.
- Thompson, James W. Employment and Crime. Department of Justice, 1981.
- Tobias, Marc W. Locks, Safes and Security: A Handbook for Law Enforcement Personnel. Charles C. Thomas Publishers, 1971.
- Traister, John. Design and Application of Security Systems. McGrath Publications, 1982.
- Trimmer, H. W. Understanding and Servicing Alarm Systems. (2nd ed.) Butterworth-Heinemann, 1990.
- Turner, Donald M. & Lesce, Tony. Watercraft Patrol and Survival Tactics. Charles C. Thomas Publishers, 1990.
- Tyska, Louis A. Controlling Cargo Theft: A Handbook of Transportation Security. Butterworth-Heinemann, 1983.
- Walker, Phillip. Electronic Security Systems. Butterworth-Heinemann, 1988.
- Weber, Thad L. Alarm Systems and Theft Prevention. (2nd ed.) Butterworth-Heinemann, 1985.

LAW ENFORCEMENT

- Kinks & Hints for the Alarm Installer. Butterworth-Heinemann, 1979.
- Albrecht, Steven & Morrison, John. Contact & Cover: Two-Officer Suspect Control. Charles C. Thomas Publishers, 1992.
- Alpert, Geoffrey P. & Dunham, Roger G. Critical Issues in Policing. Waveland Press, Inc., 1989.
- Auten, James H. Law Enforcement Driving. Charles C. Thomas Publishers, 1989.
- Bennet, G. Law Enforcement & Criminal Justice. Hugh Mufflin Publications 1979.
- Cane, Andries C. Basic Arrest and Prisoner Control Tactics: Practical Techniques-Fast, Simple, Effective. Charles C. Thomas, Publishers 1989.
- Clark, Warren E. Traffic Management and Collision Investigation. Prentice-Hall, Inc., 1982.
- Coleman, John L. Practical Knowledge for A Private Security Officer. Charles C. Thomas Publishers, 1986.
- Coleman, John L. Practical Legal Guidelines for the Private Security Officer: The Essential Consequences of the Laws Regarding Private Security and the Affective Social Trends of Today. Charles C. Thomas Publishers 1990.
- Cope, Jeff & Goddard, Kenneth. Weaponless Control: For Law Enforcement and Security Personnel. Charles C. Thomas Publishers, 1979.
- Das, Dilip K. Understanding Police Human Relations. Scarecrow Press, 1987.
- DeForest, Peter R. et al. Forensic Science: An Introduction to Criminalistics. McGraw-Hill Book Company, 1983.

- Felter, Brian. Police Defensive Handgun Use and Encounter Tactics. Prentice-Hall Inc., 1988.
- Fisher, Barry A. J. Techniques of Crime Scene Investigation. (4th ed.) Elsevier Science Publishing Company, 1987.
- Garner, Gerald W. High-Risk Patrol: Reducing the Danger to You. Charles C. Thomas Publishers, 1990.
- Geberth, V. J. Practical Homicide Investigation. Elsevier Science Publishing Company, 1983.
- Gilbert, James N. Criminal Investigation. (2nd ed.) Charles E. Merrill Publishing Company, 1986.
- Goolkasian, Gail A. et al. Coping with Police Stress. National Institute of Justice, 1985.
- Hale, Charles D. Police Patrol: Operations and Management. John Wiley & Sons, Inc., 1981.
- Hanley, Julian R. & Schmidt, Wayne W. Legal Aspects of Criminal Evidence. McCutchan Publishing Company, 1984.
- Hess, Joseph. First Move, Street Self Defense. Kendell Hunt Publications 1987.
- Holden, Richard N. Modern Police Management. Prentice-Hall, Inc., 1986.
- Iannone, Nathan F. Supervision of Police Personnel. (4th ed.) Prentice-Hall, Inc., 1987.
- Lockard, James L. Survival Thinking For Police and Correction Officers. Charles C. Thomas Publishers, 1991.
- O'Hara, Charles E. Fundamentals of Criminal Investigation. (5th ed.) Charles C. Thomas, 1985.
- Reintzell, John F. The Police Officer's Guide to Survival, Health and Fitness. Charles C. Thomas Publishers, 1990.
- Ressler, Robert K. et al. Sexual Homicide: Patterns and Motives. DC Health and Company, 1988.
- Robinson, Cyril D. Legal Rights, Duties and Liabilities of Criminal Justice Personnel: History and Analysis. (2nd ed.) Charles C. Thomas Publishers, 1992.
- Sennewald, Charles A. & Christman, John H. Shoplifting. Butterworth-Heinemann, 1992.
- Stratton, John G. Police Passages. Glennon Publishing Company, 1984.
- Swanson, Charles R. et al. Police Administration: Structures, Processes and Behavior. (2nd ed.) MacMillan Publishing Company, 1988.
- Territo, Leonard & Vetter, Harold J. Stress and Police Personnel. Allyn and Bacon, Inc., 1981.
- Thompson, George J. Verbal Judo: Words for Street Survival. Charles C. Thoams Publishers, 1983.
- Torres, Donald. Handbook of Federal Police. Department of Justice, 1985.
- Weston, Paul & Wells, Kenneth M. Criminal Investigation: Basic Perspectives. (4th ed.) Prentice-Hall, Inc., 1986.
- Wrobleski, Henry M. & Hess, Karen M. Introduction to Law Enforcement and Criminal Justice. (2nd ed.) West Publishing Company, 1986.

CRIME PREVENTION

- Carroll, John. Controlling White-Collar Crime. Designing and Auditing for Systems Security. Butterworth-Heinemann, 1982.
- Crowe, Timothy D. & the National Crime Prevention Institute. Crime Prevention Through Environmental Design. Butterworth-Heinemann, 1991.
- Duncan, J. T. Skip. Citizen Crime Prevention Tactics. U.S. Government Printing Office, 1980.
- Feins, Judith D. Partnerships for Neighborhood Crime Prevention. U.S. Government Printing Office, 1983.
- Hollander, Brian. Reducing Residential Crime & Fear: The Hartford Neighborhood Crime Prevention Program. U.S. Government Printing Office, 1980.
- Kingsbury, Arthur A. Introduction to Security and Prevention Surveys. Charles C. Thomas Publishers, 1973
- Kushmuk, James. A Re-Evaluation of Crime Prevention Through Environmental Design Program in Portland, Oregon. U.S. Government Printing Office, 1981.
- Lavrakas, Paul J. Factors Related to Citizen Involvement in Personal, Household, and Neighborhood Anti-Crime Measures. U.S. Government Printing Office, 1981.
- National Crime Prevention Council. Preventing Crime in Urban Communities. National Crime Prevention Council, 1986.
- National Crime Prevention Institute. Understanding Crime Prevention. Butterworth-Heinemann, 1986.
- National Crime Prevention Council. What, Me Evaluate? National Crime Prevention Council, 1986.
- O'Block, Robert L., Donnermeyer, Joseph F. & Doeren, Stephen E. Security and Crime Prevention. Butterworth-Heinemann, 1991.
- Poyner, Barry. Crime Free Housing. Butterworth-Heinemann, 1991.
- Poyner, Barry. Design Against Crime: Beyond Defensible Space. Butterworth-Heinemann, 1983.
- White, Thomas W. Police Burglary Prevention Programs. U.S. Government Printing Office, 1975.

INVESTIGATION

- Barefoot, J. K. Employee Theft Investigation. (2nd ed.) Butterworth-Heinemann, 1990.
- Buckwalter, Art. Interviews and Interrogations. Butterworth-Heinemann, 1983.
- Buckwalter, Art. Investigative Methods. Butterworth-Heinemann, 1984.
- Buckwalter, Art. Surveillance & Undercover Operations. Butterworth-Heinemann, 1983.
- Buckwalter, Art. The Search for Evidence. Butterworth-Heinemann, 1984.
- Carroll, John M. Confidential Information Sources - Public, Private. (2nd ed.) Butterworth-Heinemann, 1991.
- Rush, Donald A. & Siljander, Raymond. P. Fundamentals of Civil and Private Investigation. Charles C. Thomas Publishers, 1984.

Schur, Peyton B. & Broder, James F. Investigation of Substance Abuse in the Workplace. Butterworth-Heinemann, 1990.

Sennewald, Charles. The Process of Investigation: Concepts and Strategies for the Security Professional. Butterworth-Heinemann, 1981.

TERRORISM

Adams, James. The Financing of Terror. Simon and Schuster, 1986.

Aldeman, Jonathan, ed. Terror and Communal Politics: The Role of the Secret Police in Communist States. Westview, 1984.

Alexander, Yonah & Ebinger, Charles K. Political Terrorism and Energy: The Threat and Response. Praeger, 1982.

Alexander, Yonah & Ebinger, Charles K. Terrorism in Europe. Praeger, 1982.

Aston, Clive C. A Contemporary Crisis: Political Hostage-Taking and The Experience of Western Europe. Greenwood Press, 1982.

Blishchenko, I.P. Terrorism and International Law. Progress Publishers, 1984.

Cline, Ray S. Terrorism as State Sponsored Covert Warfare. Hero Books, 1986.

Crenshaw, Martha. Terrorism and International Cooperation. Institute for East-West Security Studies, 1989.

Farrell, William Regis. The U.S. Government Response to Terrorism: In Search of an Effective Strategy. Westview Press, 1982.

Goren, Roberta. The Soviet Union and Terrorism. Allen and Union 1984.

Hanle, Donald J. Terrorism: The Newest Face of Warface. Pergamon-Brassey International Defense Publishers Inc., 1989.

Janke, Peter & Sim, Richard. Guerrilla and Terrorist Organizations: A World Directory and Bibliography. Harvester Press, 1983.

Jenkins, Brian M. Terrorism & Personal Protection. Butterworth-Heinemann 1985.

Kobetz, Richard W. Target Terrorism, Providing Protective Service. International Association of Chiefs of Police, 1978.

Lakos, Amos. International Terrorism: A Bibliography. Westview Press, 1986.

Laqueur, Walter. The Age of Terrorism. Little, Brown and Company, 1987.

Laqueur, Walter & Alexander, Yonah (eds.) The Terrorism Reader (A Historical Anthology). NAL Penguin, Inc., Meridan Book-Revised Edition, 1987.

Lillich, Richard B. Transnational Terrorism, Conventions and Commentary: A Compilation of Treaties, Agreements and Declarations of Special Interest to the United States. Michie, 1982.

Marighella, Carlos. The Terrorist Classic: Manual of the Urban Guerrilla. Documentary Publications, 1985.

Melman, Youssi. The Master Terrorist: The True Story of Abu-Nidal. Adama Books, 1986.

Mickolus, Edward F. & Flemming, Peter A. Terrorism, 1980-1987 (A Selectively Annotated Bibliography). Greenwood Press, Inc., 1988.

Moris, Eric & Hoe, Alan. Terrorism: Threat and Response. St. Martin's Press, 1988.

Mullins, Wayman C. Terrorist Organizations in the United States - An Analysis of Issues, Organizations, Tactics and Responses. Charles C. Thomas Publishers, 1988.

- Poland, James M. Understanding Terrorism: Groups, Strategies and Responses. Prentice Hall, Inc., 1988.
- Quarles, Chester L. Terrorism - Avoidance and Survival. Butterworth-Heinemann, 1991.
- Rapoport, David C. & Alexander, Yonah. The Morality of Terrorism, Religious and Ethical Implications. Pergamon Press, 1981.
- Rosenthal, Uriel, Charles, Michael T. & Hart, Paul T. Coping With Crises: The Management of Disasters, Riots and Terrorism. Charles C. Thomas Publishers, 1989.
- Rubin, Barry (ed.) The Politics of Terrorism: Terror as a State and Revolutionary Strategy. John Hopkins Foreign Policy Institute, School of Advanced International Studies, 1989.
- Schmid, Alex & Jongman, Albert. Political Terrorism. Transaction Books 1988.
- Schrivver, Ronald B. & Evans, John C. & Leibstone, Marvin. Countering Terrorism on Military Installations: Final Report. Science Applications Inc., 1977.
- Scotti, Anthony E. Executive Safety and International Terrorism. Prentice-Hall Inc., 1986.
- Siljander, Raymond P. Terrorist Attacks: A Protective Service Guide for Executives, Bodyguards & Policemen. Charles C. Thomas Publishers, 1980.
- Sterling, Clarie. The Terror Network: The Secret War of International Terrorism. Holt, Rinehart and Winston, 1981.
- Stohl, Michael (ed.) The Politics of Terrorism. (3rd ed.) Marcel Dekker, Inc., 1988.
- Stohl, Michael & Lopes, George A. A State of Terrorism: The Dynamics of Governmental Violence and Repression. Greenwood Press, 1984.
- Taylor, Maxwell. The Terrorist. Brassey's Defense Publishers, 1988.
- Wardlaw, Grant. Political Terrorism: Theory, Tactics and Countermeasures. Cambridge University Press, 1982.
- Wolf, John B. Anti-terrorist Initiatives. Plenum Press, 1989.

ESPIONAGE AND COUNTERINTELLIGENCE

- Penkovskiy Papers. Ballentine 1982
- Allen, Thomas B. & Polmar, Norman. Merchants of Treason: America's Secrets for Sale from the Pueblo to the Present. Doubleday, 1988.
- Barron, John. Breaking the Ring. Houghton Mifflin Company, 1987
- Barron, John. KGB: The Secret Work of Soviet Secret Agents. Bantam, 1974.
- Barron, John. KGB Today: The Hidden Hand. Berkeley Pub, 1985.
- Barron, John & Belenko, Viktor. MiG Pilot. Readers Digest Press, 1980.
- Burrows, William E. Deep Black: Space Espionage & National Security. 1987.
- Costa, Alexandra. Stepping Down from the Star: A Soviet Defector's Story. Putnam Books, 1986.
- deBorchgrave, A. & Moss, R. Monimbo. Simon and Schuster, 1983.
- deBorchgrave, A. & Moss, R. The Spike. Avon, 1981.
- Dulles, Allen. Great True Spy Stories. Ballantine Books, 1982.

Levchenko, Stanislav. On the Wrong Side: My Life in the KGB. 1988.

Lindsey, Robert. Falcon and the Snowman: A True Story of Friendship and Espionage. 1984.

Hyde, H. Montgomery. Atom Bomb Spies. Ballantine Books, 1981.

Kessler, Ronald. Spy vs. Spy: Stalking Soviet Spies in America. McMillan 1988.

MacLean, Fitzroy. Take Nine Spies. Antheneum, 1978.

Martin, David C. Wilderness of Mirrors. Ballantine Books, 1981.

Michener, James A. Bridge at Andau. Random, 1957.

Moss, Robert. Moscow Rules. Random House (Villard Books), 1985.

Shevchenko, Arkady N. Breaking With Moscow. Alfred Knopf (hard cover); Ballantine Books (paperback), 1985.

Smith, Hedrick. Russians. Ballantine Books, 1984.

Sterling, Claire. Terror Network. Readers Digest Press, 1981.

Sutherland, Douglas. Great Betrayal: The Definitive Story of Blunt, Philby, Burgess and Maclean. Penguin, 1982.

Suvorov, Viktor. Inside the Soviet Army. Berkeley Pub., 1985.

Weinstein, Allen. Perjury: The Hiss-Chambers Case. Knopf, 1978.

Wise, David. The Spy Who Got Away: The Inside Story of Edward Lee Howard, the CIA Agent Who Betrayed His Country's Secrets and Escaped to Moscow. Random House, 1988.

Wright, Peter. Spycatcher: The Candid Autobiography of a Senior Intelligence Officer of MI5. Viking Press, 1987.

COMPUTER SECURITY

Carroll, John M. Computer Security. Butterworth-Heinemann, 1987.

Cornwall, Hugo. Data Theft. Butterworth-Heinemann, 1987.

National Research Council. Computers At Risk - Safe Computing in the Information Age. National Academy Press, 1991.

Perry, William E. Management Strategies for Computer Security. Butterworth-Heinemann, 1985.

Schweitzer, James A. Computers, Business, and Security. Butterworth-Heinemann, 1987.

Schweitzer, James A. Managing Information Security. Administrative, Electronic, and Legal Measures to Protect Business Information. (2nd ed.) Butterworth-Heinemann, 1989.

Schweitzer, James A. Protecting Information on Local Area Networks. Butterworth-Heinemann, 1988.

Stoll, Clifford. The Cuckoo's Egg. Doubleday, 1989.

MISCELLANEOUS PUBLICATIONS

The Connection, Air Force Cryptologic Support Center, C4 Systems Security Education, Training and Awareness Branch, AFCSC/SRME, 250 Hall Boulevard, Suite 347, San Antonio, TX 78243-7063, (210) 977-3154

Industrial Security Letter, Defense Investigative Service, 1340 Braddock Place, Alexandria, VA 22314-1651, (703) 325-6545

Information Systems Security Monitor, Department of Treasury, Bureau of the
Public Debt, AIS Security Branch, 200 3rd Street, Parkersburg, WV 26101,
(304) 420-6368

NSI Advisory, National Security Institute, 161 Worcester Road, Framingham, MA
01701, (508) 872-8001

Protection of Assets Manual, The Merritt Company, Dept. ASIS, 1661 Ninth
Street, P.O. Box 955, Santa Monica, CA 90406, (213) 450-7234

Sentry, Naval Criminal Investigative Service - Code 02J, Washington, DC
20388-5024, (202) 433-9096

Security Awareness Bulletin, Department of Defense Security Institute, Defense
General Supply Center, 8000 Jefferson Davis Highway, Richmond, VA
23297-5091, (804) 279-4223

Security Awareness News, Department of Defense Security Institute, Defense
General Supply Center, 8000 Jefferson Davis Highway, Richmond, VA
23297-5091, (804) 279-4223

Security Magazine, A Cahners Publication, P.O. Box 5500, Denver, CO 80217-
9888

EXHIBIT 2-5

TEST QUESTIONS

Listed below is a compilation of suggested test questions that may aid in security briefings; it is not a complete list. Test questions should be tailored to the specific material presented.

INFORMATION SECURITY

1. Individuals without a clearance need not be told what classified information is.
 - A. TRUE
 - B. FALSE
2. The best method to motivate individuals to protect classified information is to have frequent inspections.
 - A. TRUE
 - B. FALSE
3. What are the terms which designate the levels of classified information?
 - A. RESTRICTED, FOR YOUR EYES ONLY, UNCLASSIFIED
 - B. FOR OFFICIAL USE ONLY, CONFIDENTIAL, SECRET, TOP SECRET
 - C. CONFIDENTIAL, SECRET, TOP SECRET
 - D. UNCLASSIFIED, CONFIDENTIAL, SECRET, TOP SECRET
4. One requirement set forth by Executive Order 12356 is that classified material:
 - A. Be filed
 - B. Be marked with the highest classification level for its contents
 - C. Be seen only by senior personnel
 - D. Be kept in blue folders
5. A compromise of classified information is the disclosure of classified information to individuals without the appropriate security clearance or need-to-know.
 - A. TRUE
 - B. FALSE
6. An individual who is aware of the unauthorized disclosure (or compromise) of classified information can be criminally prosecuted if they do not promptly report it.
 - A. TRUE
 - B. FALSE

7. What are the two types of classification?
- A. Original and derivative
 - B. Congressional authority and General authority
 - C. Main and secondary
 - D. Depends on the size and content
8. The most frequently applied type of classification is derivative.
- A. TRUE
 - B. FALSE
9. Who is authorized to receive classified material?
- A. Personnel with security clearances
 - B. Personnel with access to the communications center
 - C. Personnel with an appropriate security clearance/need to know
 - D. None of the above
10. An individual with a Secret clearance may be given access to:
- A. Secret and Confidential information
 - B. Only Secret information
 - C. Secret and Top Secret information
 - D. Top Secret, Secret and Confidential information
11. Classified information may be disclosed to a visitor after:
- A. The visitor's identification has been verified
 - B. The visitor's clearance has been verified
 - C. The visitor's need-to-know has been verified
 - D. All of the above
12. Combinations to security containers are to be changed:
- A. When they are placed in service/taken out of service
 - B. At least once a year
 - C. When an individual no longer requires access or when it is subject to compromise
 - D. All of the above
13. Combinations to security containers are to be stored:
- A. In the telephone book
 - B. Behind your calendar
 - C. In your wallet
 - D. None of the above
14. When mailing classified material, you always place the level of classification on the outer envelope.
- A. TRUE
 - B. FALSE

15. All reproduction equipment is authorized for the reproduction of classified material.

- A. TRUE
- B. FALSE

16. Classified information for which an operational need no longer exists is to be promptly destroyed.

- A. TRUE
- B. FALSE

17. Destruction of classified information is complete when it is impossible to reconstruct or retrieve such information from the destruction process residue.

- A. TRUE
- B. FALSE

18. When procuring new security storage equipment, only Class 5 or Class 6 GSA approved security containers are authorized.

- A. TRUE
- B. FALSE

19. Even though classification markings may be applied by the drafter, the official with signature authority remains responsible for ensuring the markings are accurate.

- A. TRUE
- B. FALSE

20. What are the paragraph (portion) markings which represent the classification levels?

- A. U, C, S, TS
- B. U, R, NATO, NOFORN
- C. C, S, TS, UTS
- D. U, C, CS, TS

21. The "declassify on" line refers to a specific date or event if possible.

- A. TRUE
- B. FALSE

22. What does Originating Agency's Determination Required (OADR) mean?

- A. That you cannot look at the document without the originator's permission
- B. That you must ask the originator if you can release the information to a contractor
- C. That the originating agency must authorize declassification of the information
- D. All of the above

23. What color is the border on a SF 704 Secret cover sheet?

- A. Orange
- B. Blue
- C. Red
- D. Yellow

24. Personnel are required to report any attempts by citizens of criteria countries to cultivate a friendship or establish a relationship.

- A. TRUE
- B. FALSE

PERSONNEL SECURITY

25. The continuous evaluation program does not apply to individuals without a security clearance.

- A. TRUE
- B. FALSE

26. The granting of a security clearance is based on an investigation of:

- A. Suitability
- B. Personal integrity
- C. Trustworthiness
- D. Personality

27. An adjudicator is an individual who determines if a requested security clearance should be granted.

- A. TRUE
- B. FALSE

28. The SF 312 is the classified information nondisclosure agreement that all personnel must sign prior to having access to classified information.

- A. TRUE
- B. FALSE

PHYSICAL SECURITY

29. The three types of restricted areas are exclusion, limited and controlled.

- A. TRUE
- B. FALSE

30. A classified storage area is the only type of restricted area.

- A. TRUE
- B. FALSE

31. Physical barriers control deny, impede, delay and discourage access to areas by unauthorized persons.

- A. TRUE
- B. FALSE

32. Keys within the security key and lock control system are to be inventoried:

- A. Annually
- B. Semi-annually

33. Money and classified material may be stored in the same GSA approved security container.

- A. TRUE
- B. FALSE

34. Pilferage is the theft of property by personnel authorized within the facility.

- A. TRUE
- B. FALSE

35. Loss Prevention countermeasures include:

- A. Education
- B. Periodic inventories
- C. Random personal/vehicle inspections
- D. Key and lock control
- E. All of the above

36. The difference between the SF 701 and SF 702 is that the SF 702 is concerned with the security container, and the SF 701 is concerned with the entire area.

- A. TRUE
- B. FALSE

OPERATIONS SECURITY

37. OPSEC is the acronym for Operations Security.

- A. TRUE
- B. FALSE

38. Why should you be concerned with OPSEC?

- A. In case I'm ever an Operations Officer
- B. It might be on a service-wide exam
- C. For better community relations
- D. So that I don't give away information that would compromise an operation or a mission

39. What kind of information may need protecting?

- A. Our normal patrol route
- B. The schedule of events
- C. Which units are involved
- D. Classified operations
- E. All of the above

40. OPSEC applies only to classified information.

- A. TRUE
- B. FALSE

COMPUTER SECURITY

41. Passwords are composed of at least six alphanumeric characters.

- A. TRUE
- B. FALSE

42. To protect AIS against viruses, which of the following applies?

- A. Never introduce unauthorized software
- B. Use a scanning program
- C. Back up data
- D. All of the above

43. Which of the following are good computer security procedures?

- A. Restrict terminal access
- B. Use authorized software
- C. Respect copyright laws
- D. Change passwords frequently
- E. All of the above

44. A strong security awareness program is the key to computer security.

- A. TRUE
- B. FALSE

45. The three essential components of computer security are confidentiality, integrity, and availability.

- A. TRUE
- B. FALSE

TEST ANSWERS

1. B
2. B
3. C
4. B
5. A
6. A
7. A
8. A
9. C
10. A
11. D
12. D
13. D
14. B
15. B
16. A
17. A
18. A
19. A
20. A
21. A
22. C
23. C
24. A
25. B
26. C
27. A
28. A
29. A
30. B
31. A
32. B
33. B
34. A
35. E
36. A
37. A
38. D
39. E
40. B
41. A
42. D
43. E
44. A
45. A

CHAPTER 3. SECURITY BRIEFINGS

- A. Purpose. The security briefing is a presentation designed to persuade others and ensure all personnel understand their responsibilities for protecting government assets. Briefings should be tailored to meet the specific needs of the unit, as well as those of different groups within the unit.
- B. Responsibility. The Command Security Officer (CSO) is responsible for ensuring security briefings are properly conducted and appropriately documented. The CSO may or may not be the individual actually presenting the briefings, but his or her advice and assistance will probably be needed.
- C. Types. Listed below are the types of briefings required in the security program. Exhibit 3-1 outlines a summary and schedule of the required briefings.
1. Arrival Briefing. All personnel reporting aboard the unit shall be given an arrival briefing. The briefing shall (at a minimum) inform personnel of security points of contact, internal security procedures, Operations Security (OPSEC), loss prevention responsibilities, what classified information is, how to identify it, how and why it is protected, and actions to take if an individual discovers it unattended. Exhibit 3-2 provides a sample briefing.
 2. Access Briefing. Personnel who will have access to classified information shall be given an access briefing after receiving an interim or final clearance, but prior to being assigned duties which require access to classified information. The briefing shall inform personnel of their security responsibilities in protecting the information, including the laws applicable to the unauthorized disclosure of classified information. Exhibit 3-3 provides a sample briefing. The access briefing may be combined with the arrival briefing.
 3. Foreign Travel Briefing. Personnel (with or without access to classified information) traveling to a foreign country while on leave, authorized absence or official orders shall be given a foreign travel briefing. At a minimum, those who travel shall be briefed at least annually. The briefing shall inform personnel of general precautions for personal safety. An official debrief is not required. However, suspicious incidents shall be reported to the cognizant security manager (SECMGR) via the procedures set forth in Chapter 2 of COMDTINST M5510.21, Information Security Program. Exhibit 3-4 provides a sample briefing.
 4. Counterintelligence (CI) Awareness Briefing. Any individual who has access to classified information, and

plans to travel to or through a criteria country or to attend a meeting in the United States or elsewhere, in which representatives of criteria countries are expected to participate, shall report these plans to the unit, and shall be given a CI awareness briefing. At a minimum, those who travel or attend such meetings shall be briefed at least annually. The briefing shall inform personnel of possible exploitation attempts by foreign intelligence services and general precautions for personal safety. Exhibit 3-5 provides a sample briefing.

5. Counterintelligence (CI) Awareness Debriefing. When the individual returns, he or she shall be debriefed to provide the opportunity to report any incident - no matter how insignificant it may have seemed. Information that may have security implications shall be reported to the cognizant SECMGR via the procedures set forth in Chapter 2 of COMDTINST M5510.21, Information Security Program. Exhibit 3-6 provides a sample briefing.
6. Annual Refresher Briefing. Once a year, all personnel shall be given a refresher briefing. The briefing may address general security matters, changes in policies or procedures, specific problem areas, etc., but shall be tailored to the specific needs of the target audience. Therefore, it is not possible to provide a sample refresher briefing. Some suggested topics to cover may be OPSEC, counterintelligence reminders, reporting of possible compromises and missing, lost or stolen government property, handcarrying of classified material, crime prevention, factors affecting personnel security clearance adjudication, past year statistical data, etc. The list is endless; the intent is to tailor the briefing based on specific needs, problem areas, etc., and stimulate security consciousness by periodic re-emphasis of the basic security principals.
7. Transfer Briefing. At the time of transfer from a particular unit, all personnel who have access to classified information at their present unit shall be given a transfer briefing. The briefing shall inform personnel that their present clearance is administratively withdrawn without prejudice; all classified material must be returned; and the individual is no longer authorized access. Exhibit 3-7 provides a sample briefing.
8. Final Termination Briefing. Personnel shall be given a termination briefing upon termination of government service, or when a clearance is revoked for cause. The briefing shall remind personnel to return all classified material in his or her possession, and that they remain subject to the provisions of the criminal code and other applicable laws relating to the unauthorized disclosure

of classified information. Exhibit 3-8 provides a sample briefing.

- D. Record of Briefings. Briefings shall be recorded on the Personnel Security Record (CG-5274) for both military and civilian personnel. However, when large numbers of personnel are briefed at one time, such as for a refresher briefing or counterintelligence awareness briefing, a letter or memorandum signed by the commanding officer, with a list of personnel in attendance (such as a sailing list), may be attached to the CG-5274. The final termination briefing for civilians shall be recorded on the Security Termination Statement (DOT 1600.10).

SECURITY BRIEFINGS REQUIREMENT SCHEDULE

<u>BRIEFING</u>	<u>AUDIENCE</u>	<u>SUBJECTS</u>	<u>FREQUENCY</u>
Arrival	New employees	Security points of contact, internal security procedures, identification and protection of classified material, loss prevention responsibilities, OPSEC	Upon arrival, as occurring
Access	Employees granted access to classified information	Clearance and eligibility, classified material handling (storage, marking, transmission, destruction, etc.), attempts to solicit, reporting violations/compromises, non-disclosure agreement	Prior to granting access, as occurring
Refresher	All employees	Changes in security policies or procedures, specific problem areas, loss prevention, OPSEC, counterintelligence reminders, etc.	Annually
Foreign Travel	Employees traveling to a foreign country	Hotel/vehicle/airline security, personal safety, travel advisory hotline, terrorism awareness	As required
Counterintelligence Awareness	Cleared employees traveling to or through a criteria country (or attending a meeting)	Foreign intelligence exploitation, attempts to solicit, contacts, approach techniques, security precautions, personal safety	As required

SECURITY BRIEFINGS REQUIREMENT SCHEDULE

EXHIBIT 3-1

<u>BRIEFING</u>	<u>AUDIENCE</u>	<u>SUBJECTS</u>	<u>FREQUENCY</u>
Counterintelligence Awareness Debriefing	Cleared employees returning from a criteria country (or a meeting)	Any incident of a suspicious nature, e.g., attempts to establish a friendship, attempts to obtain information, etc.	As required
Transfer	Employees transferring from the unit	Clearance and eligibility, return of classified material, divulging, attempts to solicit	As occurring
Final Termination	Employees leaving government service or when clearance is withdrawn/revoked	Return of classified material, divulging, attempts to solicit, criminal sanctions, non-disclosure agreement	As occurring
Continuing Security Awareness	All employees	Posting of signs, posters, newsletters, plan of the day/week reminders, security awareness day/week/month, pamphlets, cartoons, puzzles, video tapes, etc.	Continuously

EXHIBIT 3-2

ARRIVAL BRIEFING

INTRODUCTION

Welcome! A special congratulations on your new assignment. Your job makes you a member of a very special team comprised of military and civilian personnel who are engaged in work which impacts the defense of our great country.

In performing your job, you will be dealing (at a minimum) with unclassified sensitive information. You may also be working with information which has been classified in the interest of our national security - that is, information which is CONFIDENTIAL, SECRET, OR TOP SECRET. Security should become a vital part of your daily routine and it is essential you know and understand the requirements for protecting government assets (classified information, property and personnel).

I mentioned you are part of a team. I know in some area of your life you have learned how important teamwork is to the final outcome of any event. Every individual must do his or her part if the team is to win. And this team must win. We have established a security program to protect government assets and prevent our adversaries from gaining access to sensitive information. However, no matter how comprehensive the program may be, the key ingredient is people. You and your coworkers will ultimately determine the success of our established procedures. Your daily security vigilance helps us keep our national security advantage and protects the freedoms we all enjoy so much.

NOTE: At this time, inform the individual of security points of contact at the unit; e.g., Command Security Officer (CSO), Classified Material Control Officer (CMCO), Area and District Security Manager (SECMGR), Unit Automated Data Processing Systems Security Officer (ADPSSO), etc. Advise them of other information specific to the unit, e.g., where security regulations can be located, where to report security incidents, etc.

PERSONNEL SECURITY

Personnel Security is the system by which we assure that everyone employed by the Coast Guard meets certain standards. Prior to reporting to work, unless you transferred from a Coast Guard unit or other government agency, you were asked to fill out certain forms concerning your background. An appropriate investigation was conducted to determine your suitability for employment with the Coast Guard, and to determine your eligibility for a security clearance (if required). Not every employee will require a security clearance. A person with a security clearance at one unit may transfer to another unit and not be issued a clearance, or may be granted a clearance at a level lower than the one previously held. It all depends on the needs in your current position.

Questionable information collected during the investigation must be clarified and may require further investigation. The information obtained must be evaluated and a common sense determination made taking into consideration all available information. Questionable factors include criminal conduct, alcohol abuse, drug abuse, financial irresponsibility, and falsification of information provided in interviews or on employment forms, or any other factor that would cast in doubt an individual's responsibility, loyalty, reliability or trustworthiness.

Evaluation of your character and activities doesn't end after the initial investigation. We have a program which requires a continuing evaluation of your eligibility to hold a security clearance. Your actions can affect your ability to retain a security clearance, and possibly your position. We've learned that one of the greatest threats to our security comes from our own carelessness and complacency.

It takes your cooperation to make this continuous evaluation program work. You have a responsibility to report to your CSO any questionable information that indicates an individual no longer meets the security standards for eligibility to hold a security clearance. You may feel a little uncomfortable about reporting a coworker, but keep in mind the importance of security interests, as well as national security interests, and the good of the entire country. If that person is compromising Coast Guard security, it affects not only the whole U.S. security program, but you and your family as well.

INFORMATION SECURITY

Executive Order 12356 prescribes a uniform system for safeguarding national security information. Classified information is official information that requires protection against unauthorized disclosure in the interest of national security. Unauthorized disclosure occurs when someone who is not authorized by the government to have access to classified information does get access, either accidentally or intentionally.

Access to classified information is permitted only to persons who possess an appropriate security clearance and an official need-to-know. Your position may or may not require access to classified information. If it does, further information will be provided to you during an "access briefing". If not, this section is provided in case you inadvertently discover unprotected classified material, you will be able to identify it and properly protect it.

There are three categories of classified information that require specified protective measures; the unauthorized disclosure of this information will result in a degree of damage to the national security:

- TOP SECRET - The unauthorized disclosure of this information could reasonably be expected to cause "exceptionally grave damage" to our national security.

- SECRET - The unauthorized disclosure of this information could reasonably be expected to cause "serious damage" to our national security.

- CONFIDENTIAL - The unauthorized disclosure of this information could reasonably be expected to cause "damage" to our national security.

All documents containing classified information will be marked in a prescribed manner to indicate the classification assigned and the degree and duration of protection required. Classification levels will be conspicuously marked or stamped at the top and bottom of all pages. Paragraphs, subjects and titles will be individually marked with parenthetical symbols (TS), (S), or (C). The face of the document will also include "Classified by" and "Declassify on" lines to identify classification sources and declassification and downgrading instructions.

Classified material will be stored in approved secure areas, in GSA approved security containers or under the direct observation of authorized personnel. If by chance, you discover classified material unprotected, i.e., in an incoming mail box, in a copier machine, on top of a file cabinet, on a desk, etc., you have an immediate responsibility to protect the material from further risk and report the incident to your CSO. If you cannot both protect the information and report the incident, have someone else make the report while you continue to protect the information.

If you are approached by anyone seeking unauthorized access to classified or sensitive information, immediately report it to your CSO. It is no secret that dedicated foreign intelligence services are working in this country to gain valuable information. Compromised classified information could severely damage America's national security; we must all work together to prevent this from happening.

LOSS PREVENTION

Care must be taken to ensure that adequate safeguards are established to protect government property from loss or theft. Items considered to be highly susceptible to loss or theft include calculators, small office machines, transistor radios, desk clocks, postage stamps, etc. Government funds, controlled medical substances, arms, ammunition and explosives, sensitive forms such as unissued identification cards, purchase orders, and credit cards are also highly susceptible to loss or theft. Careless handling of these items encourage thievery or contributes to their inadvertent loss.

Concern is not only focused on the external threat of criminal activity; it is specifically directed toward the internal threat: theft and pilferage by those who have authorized access, inattention to physical security practices and disregard for property control and accountability.

You have a responsibility to immediately report to your CSO any missing, lost or stolen government property. Timely reporting increases the possibility that property will be recovered. Reporting losses provides a measure of effectiveness for internal controls, stimulates reviews of inventory and accountability procedures, and reflects both strengths and weaknesses in the security program.

You can support the loss prevention effort by observing the following precautions:

- Lock up all small items at the close of business.
- Do not leave money or other valuables in desk drawers.
- Keep your purse or wallet with you at all times.
- Make sure coat/clothing racks are well within controlled spaces, not close to exterior doors or open hallways.
- Require all unknown persons who enter your space to identify themselves. Verify their reason for being there if you are not sure.
- Report missing, lost or stolen government property, including identification badges and keys.
- If you observe any suspicious persons or activities in buildings, parking areas, etc., immediately report it to your CSO.

OPERATIONS SECURITY

Operations Security (OPSEC) is a process which identifies what sensitive information needs protecting, where the information can be vulnerable to collection by an adversary, and what actions we can take to protect information related to our projects, plans and operations. OPSEC is concerned with the protection of all information which could be useful to a known adversary. We must recognize that information can be gathered through written and verbal communication, visual observations, and technical intelligence gathering methods.

The OPSEC process looks at the entire operation and the threats, vulnerabilities and the countermeasures associated with a project, program, exercise or operation. The process pays particular attention to how we do things. It considers all the traditional programs and defines weaknesses not collectively addressed by those programs.

OPSEC planning efforts are coordinated with OPSEC representatives, technical employees, and security specialists. During planning, the OPSEC process identifies information requiring protection and the detectable activities which may reveal the information we want to protect. Detectable activities are considered vulnerabilities which require countermeasures.

You can support the OPSEC effort by being aware of what information you need to protect, complying with OPSEC instructions and plans, and coordinating OPSEC issues with your OPSEC representatives.

CONCLUSION

Security's mission is to establish an awareness of good security practices on the part of all employees and to ensure compliance with government policies and procedures designed to protect classified information, property and personnel. Security is here to help you. Here's how you can help us:

- Understand your individual security responsibilities.
- Make security a daily habit.
- Ask if you have any questions, or need help.

Security depends on your cooperation and personal awareness. You are asked to take an active part in protecting your country's vital secrets, property and personnel. You are asked to keep your sense of security awareness strong. You must choose to do what you know is right, now and for the future.

EXHIBIT 3-3

ACCESS BRIEFING

INTRODUCTION

Competent authority has determined that you require access to classified information in the performance of your official duties. You are now in a position of high public trust. As a government employee, the standards of conduct required of you are higher than for other U.S. citizens. Your conduct reflects not only on you personally, it also reflects on your unit and the Coast Guard. The trust placed in you should be exemplified by your daily efforts as a member of our security team.

Access to classified information is permitted only to persons who possess an appropriate security clearance and who have an official need-to-know. Access means the ability and opportunity to obtain knowledge or possession of classified information.

A security clearance is an administrative determination, based on an appropriate investigation, that you are trustworthy and eligible for access to classified information. If you have been granted a TOP SECRET clearance, you are eligible for access to Top Secret, Secret and Confidential information. If you have been granted a SECRET clearance, you are eligible for access to Secret and Confidential information. If you have been granted a CONFIDENTIAL clearance, you are eligible for access to Confidential information only.

Whether you are given access depends on the information you need-to-know to do your job. Need-to-know is a determination that you have a requirement for access to classified information to accomplish your official duties. You are not only responsible for restricting your own access to that which you need-to-know, but also for making sure that others are properly cleared and have a need-to-know before you release the information to them.

ORIGINAL AND DERIVATIVE CLASSIFICATION

There are two types of classification, Original and Derivative. Original classification is the initial determination that information requires protection in the interest of national security. Original classification is only required when new information is developed which cannot reasonably derive its classification from other classified or related information. Only those officials who have been specifically delegated original classification authority (in writing) may make original classification decisions. Remember, in peacetime, only Commandant (G-C) and (G-O) have original classification authority.

Derivative classification is simply classifying information based on a previous original classification decision. Your information may be derived from an original classification action, from a classified source document or classification guide. You may be incorporating, paraphrasing, summarizing, or restating that information, but your classification is a result of that previous

original classification decision, and is therefore, a derivative classification.

Remember that information should be classified at the lowest appropriate classification level and should be downgraded (classification lowered) or declassified (classification removed) at the earliest possible date.

MARKING

All documents containing classified information shall be marked in a prescribed manner to indicate the classification level assigned and the degree and duration of protection required. The main purpose of marking is to ensure that there is no doubt in the user's mind as to the classification of the specified material. These markings are the very minimum required for classified documents. COMDTINST M5510.21, Information Security Program, contains more detailed marking instructions and notices.

The overall classification shall be conspicuously marked or stamped on the face and back cover of the document. Each interior page shall be marked at the top and bottom with the highest classification of information on that page, or with the overall classification of the entire document.

Each paragraph shall be marked to show the level of classification or that it is unclassified. The parenthetical symbols (TS) for Top Secret, (S) for Secret, (C) for Confidential, and (U) for Unclassified shall be placed immediately preceding the text it governs. Subjects or titles shall also be marked immediately following and to the right of the subject or title with these parenthetical symbols.

Each face of a classified document shall be marked to show the name and title of the classifier, the source of classification, and the date for any downgrading or declassification action.

SAFEGUARDING

All classified material received or transmitted by the unit shall be processed through a designated Security Control Point (SCP) for accountability purposes. The SCP prepares receipts and accountability records and forwards the classified material to the proper office for the necessary action. However, YOU are the key player in this system. All the records and receipts are meaningless unless YOU know how to safeguard the information. Some important points to remember:

- Only persons with an appropriate security clearance and need-to-know are authorized access to classified information.
- Classified material shall be stored in approved secure areas, in GSA approved security containers or under the direct observation of authorized personnel.

- Security container combinations shall be protected the same as classified material and stored appropriately (never in wallets, desks, calendars, etc.) Combinations shall be changed as often as necessary, but at least annually. Only a minimum number of people shall have access to the combination.

- When removed from storage, classified documents shall have a standard form cover sheet (SF 703, 704, 705) attached.

- Classified information shall not be read or discussed in public places or in the presence of unauthorized personnel.

- Contrary to popular belief, there is no requirement to only discuss classified information in a designated classified space. It would be unreasonable to expect two employees sharing an office and working on the same project not to talk about what they are doing and go to a classified space. What is required is that employees take reasonable precautions to ensure that only authorized ears hear what is discussed. Look around to see who is within hearing range. Never have discussions near open doors or windows, or when someone is using the telephone.

- Non-secure telephones continue to be the most widely exploited communications instrument; continuous caution and awareness of their vulnerabilities is a must. Classified discussions over non-secure telephones is prohibited. Telephones and telephone systems are subject to communications security monitoring. Classified discussions shall only be over approved telephone systems, e.g., the STU III. Use of the STU III is also encouraged when discussing sensitive information and operational matters.

- Reproduction shall be held to an absolute minimum and only on authorized machines. Reproduced copies shall be controlled and accounted for the same as original documents.

- Classified material shall be destroyed when there is no longer an operational need for it. COMDTINST M5600, Directives, Publications and Reports Index, will aid in determining holding requirements. Security containers are expensive and accountability procedures are time consuming; the less classified material you have the better.

- A system of double security checks (utilizing SF 701) shall be employed at the close of business to ensure all classified information is properly secured.

- Classified material shall not be removed from the unit unless specifically authorized by the commanding officer. It shall never be taken home.

- Transmit classified material only by approved methods. Only handcarry it when it is not available at your destination or when time or other constraints dictate. This practice is generally discouraged due to concerns of hijacking, accidents and human error (e.g., forgetting briefcases). Rather than handcarry the material on your return trip, mail it back to your unit.

ADMINISTRATIVE SECURITY DISCREPANCIES AND COMPROMISES

Administrative security discrepancies are, in simple terms, not following security regulations/procedures. They fall under two categories: Those that result in a compromise or possible compromise of classified information, and those in which security regulations/procedures have been violated but do not result in a compromise or possible compromise.

A compromise is simply disclosing classified information to anyone who does not have the appropriate security clearance or need-to-know. Another term for compromise is unauthorized disclosure.

Everyone would prefer to avoid these infractions, but they happen in the best of places. And when they happen, you have the responsibility to immediately report the incident to your Command Security Officer (CSO).

These infractions must be vigorously investigated so that the cause can be identified and corrected; and we can determine what damage may have been done and take appropriate actions to minimize the damage. Timely reports, reflected through inquiry and conscientious corrective action, will be recognized as one of the best indicators of a security-conscious work force and a well-managed security program.

TRAVEL TO FOREIGN COUNTRIES

You have the responsibility to notify your CSO prior to any travel outside the U.S. so that you may be given the proper security briefings. These briefings will inform you of general security precautions, safety tips, and possible intelligence-gathering methods and potential hazards you may be exposed to.

THE FOREIGN INTELLIGENCE THREAT

The foreign intelligence threat arrayed against the U.S. is pervasive and confronts the government and our nation's industry with increasingly serious challenges. This threat continues despite the end of the Cold War. Foreign intelligence services depend to a large degree on their human collection networks throughout the world to satisfy their requirements for U.S. advanced technology. Persons are recruited, or volunteer, to provide information to foreign intelligence services.

You have the responsibility to report to your CSO any attempts by any unauthorized individual to solicit classified or sensitive information. Additionally, you must report to your CSO any attempts by representatives of criteria countries to:

- Establish a personal or professional relationship.
- Obtain information through monetary payments, bribery, observation, collection of documents, or by personal contact.
- Coerce personnel by blackmail, threats against or promises of assistance to relatives living under their control.

- Exploit discontented personnel or those with personal difficulties.
- Intimidate, harass, entrap, discredit, search, spy on, or recruit personnel.
- Induce personnel to defect or induce those who have fled from another country to redefect.

NONDISCLOSURE AGREEMENT (SF 312)

You will now be asked to sign the SF 312 as a condition of access to classified information. The SF 312 is a contractual agreement between the U.S. Government and you, in which you agree to never disclose classified information to an unauthorized person (now or beyond your employment with the Coast Guard).

Its primary purpose is to inform you of the trust that is placed in you by providing you access to classified information; your responsibilities to protect that information from unauthorized disclosure; and the consequences that may result from your failure to meet those responsibilities. If you knowingly, willfully, or negligently disclose classified information to unauthorized persons, you are subject to a wide range of administrative sanctions, civil remedies, and criminal prosecutions.

NOTE: The SF 312 is to be signed only upon first time access to classified information, or if previously unexecuted.

EXHIBIT 3-4

FOREIGN TRAVEL BRIEFING

Planning a trip overseas is always worrisome. Whether for official travel or pleasure, we worry about what to take and what not to take; tickets, passports, money, etc. Recently, we've had another worry - terrorism. Throughout the world, terrorism has become a means whereby weaker governments or political groups try to force their beliefs and goals upon others. International terrorism is REAL and has touched the lives of many Americans when least expected. However, terrorism is not the only problem overseas travelers face today. Death and injury also occur during acts of random violence spawned by ethnic differences, extremism, fundamentalism, political violence, poverty and tribalism. We cannot make ourselves immune from terrorism anymore than we can from ordinary criminal violence. But the same precautions taken in a personal crime prevention program will serve to deter terrorist as well.

The information presented in this briefing is for your personal safety. Security must be implemented to ensure continued safety in foreign environments. Each country and each circumstance will present you with a unique situation. Individual precautions can substantially reduce the possibility of a successful criminal or terrorist attack and could make a difference in your survival.

BEFORE YOU GO

- Being self-informed is important. Learn about your destination, its history, culture, local customs and laws. This can be done by consulting your local travel agent, library, or talking to people who have been there.
- Call the State Department travel advisory hotline at (202) 647-5225. The hotline provides up-to-date information concerning potential threats to Americans generated by political disorder, crime, health risks, and other possible problems that travelers may face.
- Check the calendar. Terrorists often carry out attacks on days commemorating significant events in their regions, religious holidays or on anniversaries of previous attacks.
- Choose your airline carefully. Some are more likely to be targeted than others. The safest airlines tend to be those from such countries as Sweden, Switzerland, Singapore and Hong Kong, (which are not members of political blocs or embroiled in localized conflicts).
- All references during travel arrangements should be made without military rank.
- Try to fly on a larger plane if possible (747, DC10). Skyjacking a larger plane requires more planning, manpower and effort.

- Coach is safer than first class. Terrorists tend to use first class as their command post. You would be closer to them if they decided to open fire. Should there be a rescue attempt, you run a greater risk of being caught in a crossfire. It's easier to blend into the crowd in coach.

- Avoid aisle seats. Passengers on the aisle are generally subjected to the most abuse. If a rescue operation takes place, most of the shooting would be directed down the aisles.

- In the event your return is delayed, make sure your personal matters are in good order and accessible to your spouse (or designee) prior to your departure, e.g., power of attorney, insurance policies, important papers, safe deposit box, joint bank accounts, updated will, etc.

- Before leaving, you may want to have a frank discussion with your family concerning appropriate actions in the event your return is delayed.

LUGGAGE AND PACKING

- Travel light. Take what you'll need, but nothing more.

- Don't take flashy clothes or jewelry that will draw unnecessary attention to yourself.

- Avoid packing anything that is breakable, high value, indispensable or of sentimental value. Don't take anything you can't afford to lose.

- Have your name and address (never with your military affiliation) on the inside and outside of each piece of luggage.

- Pack eyeglasses and important documents in a small carry-on piece of luggage and keep it with you.

- Leave official orders or papers in your checked in luggage and not on your person.

- Only take essential identification with you (passport, shot records, drivers license, military ID, etc.). Leave building passes, security badges, military club cards, etc. at home.

- Don't advertise your religious, ethnic or military affiliation. Don't wear or take distinctively American apparel or clothing with military patches or insignia. Keep tattoos covered.

- Have an ample supply of all necessary prescription medications in your carry-on luggage. In addition to the normal risk of separation from your checked luggage, this precaution could be a lifesaver if you have to endure a long hijacking. Keep medicines in their original labeled container to make customs processing easier. Also carry a card specifying your blood type and necessary medical information.

AT THE AIRPORT

- Don't linger in the main terminal area. Airport crowds repeatedly have been targeted by terrorists who simply open up with automatic weapons and grenades. Check in quickly, go through immigration and security checks, and wait in a secured passenger area for your flight.
- Check your bags at the counter, not at the curbside. Lock them to prevent someone from slipping drugs or a bomb inside. If a stranger asks you to carry something aboard the plane, refuse and notify appropriate security officials.
- Avoid discussing official business within hearing of other passengers. Do not address each other by rank.
- Sit with your back to a wall. This way you can see everything that's going on.
- Avoid sitting near windows. Try to stand or sit near pillars that provide cover. Be aware of your surroundings. Notice vending machines, sofas and other objects that you could duck behind.
- Stay away from unattended bags. Also avoid trash bins, telephone booths and other enclosures that could contain an explosive device.
- If caught in an open area during a terrorist attack, the best action to take is to immediately drop to the ground and pull your arms over your head the instant you hear shooting or explosions.
- If anything looks suspicious, notify authorities. It is amazing how often passengers have picked out terrorists and hijackers in their midst before an attack occurs but didn't say anything for fear of offending the person. Most Americans are too polite. Don't be bashful about any passenger who behaves peculiarly or looks out of place.

IN THE AIR

- Once seated, be sure to identify the location of the emergency exits.
- On a foreign carrier, avoid speaking English as much as possible. Sit quietly and don't draw attention to yourself.
- Memorize your passport number and other essential information in order to avoid flashing your passport around when filling out landing cards.
- Keep your seatbelt on. If a bomb goes off in the plane there will probably be sudden decompression in the cabin, with people and objects being drawn toward the hole.
- Some airlines carry sky marshals. They may attempt to prevent a hijacking. Be prepared to drop to the floor or to scrunch down and cover up if gunfire starts. Whatever you do, don't stand up and look around.

- Don't give hijackers any reason to mistake you for a sky marshal. Not all of them may reveal themselves at first. They may remain seated among the passengers, ready to "neutralize" anyone who makes a sudden movement.

- Don't do anything to call attention to yourself. This is the most important rule for surviving a hijacking. Try not to make eye contact with any of the terrorists. Don't complain, protest your detention or destination and don't ask questions. Make yourself inconspicuous. Maintain a neutral composure; give passive cooperation, don't show fear or anger. Only if you require medication or have some other severe medical problem should you let your captors know about you.

- Don't try to reason with your captors. If they are desperate enough to hijack an aircraft, they are capable of reacting unpredictably to the slightest provocation. Take their abuse without complaint. Don't do anything that will force them to react thoughtlessly, out of their own anger or fear. Should you antagonize them, they may single you out for retribution.

- Don't attempt to gain favor with the terrorists. They generally have little respect for those who grovel. Recognize your responsibility to the other passengers.

- Expect to be uncomfortable; an aluminum cylinder parked on an airport runway can get very hot in the summer and very cold in the winter. You will likely be cramped and stiff. The stench will probably become unbearable. The passengers may not be permitted to use the restrooms and may have to relieve themselves in their seats.

- Take a mental picture of the situation inside the plane. If you are released or escape, authorities will want to know the number of hijackers; their descriptions (gender, nationality, clothing, language); any routines they have established; and the location of hijackers, hostages and weapons or explosives.

- Be alert for possible rescue attempts. Should you hear noises outside the aircraft, don't stare out the window. Get down in your seat and be ready to cover your head or shield your children.

- Don't get involved in a rescue operation, just follow orders. Whatever you do, don't pick up a stray weapon. The assault team may mistake you for one of the hijackers; they will shoot first and ask questions later.

- Watch for terrorists trying to blend in with the passengers if shooting starts. One of the hijackers of an Egypt Air flight to Malta tried to escape by posing as a passenger. Until the situation is under control, the rescuers are likely to treat you roughly. You may be searched. Don't be offended. Comply.

MONEY

- Before you leave, exchange some money for use immediately after you arrive.

- Never exchange money with strangers on the street. It is probably illegal and you could end up in jail.
- Never countersign a travelers check until the moment you're ready to cash it. Each time you cash one, record the number, date and where you cashed it. This is important for a quick refund if lost.
- Carry cash, checks, credit cards and identification on different parts of your person. Money belts are recommended.
- If you are traveling with someone, divide the wealth; each person should carry a portion of the money, travelers checks, credit cards, etc.

HOTELS

- If possible, select a room between the second and eighth floors (too high for easy outside entry and low enough for fire/rescue equipment).
- Better hotels usually have good security and their own security staffs.
- Always keep your windows and doors locked; make a safety check before retiring to ensure they are properly locked.
- Identify emergency exits and stairwells. Know where to locate and how to use the fire extinguisher.
- Make good use of the hotel safe. Put your valuables in the safe and get a receipt for them.
- Don't leave anything of value in your room when you go out, even if it is locked in your suitcase. Don't use a travel lock to secure a drawer containing valuables. It will tell a thief where to look.
- Keep your room in a neat and orderly fashion so you can detect tampering or out of place objects.
- When you leave your room, don't leave indicators showing you are out. Don't tape notes on your door, and don't put a "please make up room" type of sign on the door.
- When out, leave a light on or a radio/TV playing low, in order to deter burglars.
- After dark, keep your curtains and blinds closed. Avoid frequent exposure on balconies.
- Do not answer the phone with your name. Avoid hotel paging.
- Be careful when answering the door; do not answer it automatically. Check by observing through the "peep hole" or an adjacent window.

WALKING

- Avoid walking or jogging alone. Use the "Buddy System". Vary your route.
- Avoid sitting at a sidewalk cafe table or by a window. Know where the emergency exits are.
- Avoid public demonstrations, accidents and other civil disturbances. Ignore taunts and obscene gestures.
- Shun publicity, especially the local news media.
- Do not discuss personal matters such as your travel plans or business dealings with people you don't know.
- Learn useful foreign phrases to request assistance (police, medical, U.S. Embassy, etc.). Keep a phrase book handy.
- Know how to use the local telephones and keep the required coins with you for a pay phone.
- Keep a list of important local phone numbers with you such as police, hotel and U.S. Embassy.

VEHICLE SECURITY

- Vary modes of public transportation whenever possible.
- If possible, choose your own taxi. Use various taxi companies on a random basis. Wait for them indoors if possible. Specify the route you want the taxi to follow.
- In renting a vehicle, select a plain car, minimize the "rich American look". Consider not using a government vehicle that announces its occupants status.
- Safeguard vehicle keys.
- Pay attention to vehicle maintenance. Correct any noted problems that could cause the vehicle to stall. Ensure tires have sufficient tread.
- Keep gas tank at least 1/2 full at all times.
- Prior to getting into the vehicle, check beneath it, looking for wires, tape or anything unusual. Look for scuffs on pavement that could indicate someone was underneath the vehicle. Display the same wariness before exiting your vehicle.
- Avoid late night travel. Avoid known danger areas, isolated roads and dark alleys.
- If you have a driver, develop a simple signal to be used in case of trouble.
- Travel with companions or in a convoy when possible.

- Check the reliability of permanently assigned drivers.
- Attend special defensive driving training if available.
- When parking vehicles, secure car doors and lock garage doors.
- Habitually ride with seatbelts buckled, doors locked, and windows closed.
- Do not allow your vehicle to be boxed in. Keep a minimum of eight feet between your vehicle and the one in front of you.
- Be alert for surveillance or danger while driving or riding.
- Know how to react if surveillance is suspected or confirmed. Do not stop or do anything to confront suspected surveillance. If possible, get a description of the car and its occupants. Drive to the closest safe haven and report it immediately to appropriate security officials.
- If your vehicle is under attack, attempt the following: Without subjecting yourself, passengers, or pedestrians to harm, try to draw public attention to your car (flash lights, sound horn, etc.). Put another vehicle between you and your pursuer. Execute an immediate turn and get out of the attack zone. If the road is blocked by terrorists vehicles...don't stop! Ram the blocking vehicle if necessary. Hit near rear fender of blocking vehicle at full power and drive thru. Don't take your foot from the accelerator. Go to the closest safe haven and report the incident immediately to appropriate security officials.
- Do not stop to assist another vehicle which appears to be broken down. Call and report it to the local authorities.

HOSTAGE SURVIVAL

The totally unpredictable nature of terrorism makes it impossible to be 100% secure. The possibility always exists, no matter how slight, you or members of your family will become victims of a terrorist incident regardless of how many precautions you take or how diligently they are followed. The following suggestions and guidelines have been obtained from people who have survived terrorist hostage or kidnapping situations and have witnessed the murders of those who have not survived.

- Stay calm and have faith; maintain your dignity and self-respect. Do not display bravado or cowardice.
- Stay alert for possibilities for escape. Ensure the odds of success are in your favor or do not attempt it.
- Be certain you can explain everything on your person.
- Do not criticize or antagonize your captors.
- Be prepared to be accused of being a member of the Central Intelligence Agency (CIA) or other intelligence organization.

- Make a mental note of everything that goes on - sounds, descriptions, times, phone numbers, etc. Leave evidence at all locations you are taken to assist police in their search. Do this only if it will not endanger you.
- Anticipate isolation and other methods to break or disorient you.
- Attempt to locate yourself as far away from your captors as possible. Should police attempt a rescue, you will be out of the line of fire.
- Set up a schedule of mental and physical activity and follow it.
- Comply with all instructions as well as you can.
- Don't be afraid to ask (don't demand) for anything (e.g., books, paper, medical attention, etc.)
- Eat whatever they give you and do not refuse any favors.
- Beware of a possible unconscious shift in your loyalties to your captors.

The likelihood of becoming a hostage is slim; however, you must be prepared to survive the ordeal should it happen. An important point to remember is that the longer you are held, the greater your chance of surviving.

ASSISTANCE ABROAD

U.S. Consular officers are located at U.S. Embassies and Consulates in most countries abroad. Consular officers can advise you of any adverse conditions in the places you are visiting and can help you in emergencies. If you plan more than a short stay in one place, it is advisable to register with the nearest U.S. Embassy or Consulate. This will make it easier should someone at home need to urgently locate you or in the unlikely event that you need to be evacuated due to an emergency. It will also facilitate the issuance of a new passport should yours be lost or stolen. Should you find yourself in any legal difficulty, contact a consular officer immediately. Consular officers cannot serve as attorneys or give legal advice but they can provide lists of local attorneys and help you find legal representation. Consular officers cannot get you out of jail. However, if you are arrested, ask permission to notify a consular officer - it may be your right. American consular officers will visit you, advise you of your rights under local laws, ensure that you aren't held under inhumane conditions, and contact your family and friends if you desire. They can transfer money, and will try to get relief for you, including food and clothing in countries where this is a problem.

A FINAL WORD

Now that you are aware of the basic precautions which should be taken during your trip, take some time to put all of this information into perspective. We have fulfilled our requirement to brief you. If you follow these precautions and use your own good common sense, you will reduce the risk of encountering problems; but remember, carefulness need not become an obsession. This is YOUR trip. Enjoy it!

COUNTERINTELLIGENCE (CI) AWARENESS BRIEFING

You must have a hundred things on your mind before your trip abroad, but I'm going to add to your mental baggage today with some serious thoughts on a serious subject. The foreign intelligence threat to U.S. military and civilian personnel continues despite the end of the Cold War. Personnel are now, more than ever, communicating with foreign nationals from all over the world. Foreign intelligence services make it their business to learn the identities of Americans. Their main objectives are to induce Americans to either willingly or unwillingly reveal U.S. defense, security, law enforcement, industrial, scientific and technical information and/or to recruit them, through compromise and blackmail, to collect information for them upon their return to the U.S.

Travelling to or through criteria countries (listed in Enclosure (3) to COMDTINST M5510.21, Information Security Program), you will be in a position for possible exploitation attempts - because you are an American who has access to classified information, because you will be operating on unfamiliar ground, and because you probably aren't convinced that YOU could ever be of interest to foreign intelligence. Well, chances are you haven't ever been targeted by a foreign intelligence service, but they are always on watch for any American who may cooperate with them. I certainly don't intend to frighten you, or dissuade you in any way from your journey, but you have to be doubly careful that you don't place yourself in jeopardy.

- Visa applications are routinely scrutinized by intelligence services to determine your immediate or future value to their intelligence operations. In order to avoid possible difficulties in this area, it is important that you fill out the forms truthfully and accurately. It is especially important that you name any relatives that you intend to visit in the host country.

- When obtaining visas, travelers should ask the appropriate consular office how much foreign currency (U.S. and other) and what valuables may be taken in and out of the countries to be visited. You may not be allowed to import local currency into the country you are visiting. Make sure you have enough money for the trip, and strictly follow the approved itinerary. Never exchange money with strangers on the street.

- You may wish to carry gifts for friends or relatives with you. Items to be carried as gifts should be neither controversial nor prohibited. Do not bring pornography, narcotics or political material. Pornography laws of many countries are far stricter than those in the U.S., and you should avoid taking any magazines or other materials that might be considered pornographic. Any over-the-counter or prescription drugs should be in a clearly marked container and in reasonable quantities to convince authorities that they are for your personal consumption.

- Do not carry with you (on behalf of a third party) any letters, messages, or packages for private individuals. You may be deemed guilty of circumventing normal channels of communication, or you may be regarded as a courier for illegal or subversive purposes.
- It is unwise for you to drive in some criteria countries. Try to use public transportation or hire a driver, as local traffic regulations may be confusing.
- Assume that your hotel room is equipped with listening or recording devices. Do not search for such devices, and do not make an issue of it if you should by chance find one. The presence of such equipment may not be significant as it may not specifically concern you. Do not try to neutralize such devices by running tap water, playing your radio, etc. Overt efforts on your part to combat such penetration will only make you more suspicious to the intelligence services. The best defense against such devices is to avoid political or sensitive discussions. Should you discover any device of the above kind, take no overt action against it. Continue your normal conversation, giving no indication that you have discovered it. Report it to the nearest U.S. Embassy or Consulate and to your Command Security Officer (CSO) during the Counterintelligence (CI) Awareness Debriefing (upon your return).
- Beyond your hotel room, you should assume that conversations in vehicles, train compartments, restaurants, conference rooms and other public places may be monitored. It is technically possible to monitor your conversations in open, outdoor areas; however, those areas are normally more secure than indoor locations.
- Avoid unnecessary discussions concerning your job, your work place and other official matters. Also avoid discussing other U.S. employee's habits, character or other matters which reveal weaknesses or idiosyncrasies.
- Assume that your personal luggage will be searched at some time in your hotel room. If you discover evidence of this, do not make a big issue of it. Positive evidence of such activity, however, should be reported to the nearest U.S. Embassy or Consulate and to your CSO during the CI debriefing. It is just as well not to bother locking your luggage, as most locks can be easily picked. If the lock cannot be picked, this will only increase the curiosity of the intelligence agent and the lock may be broken. Never leave your luggage unattended if it contains valuable papers or documents you do not wish anyone else to read. If you surprise someone searching your possessions, don't take any violent or physical action, but report the incident to appropriate security officials.
- You may receive a wrong number or otherwise mysterious telephone call in your hotel room at any hour of the day or night. Don't let this unduly upset you. It may be a crude but effective method of determining whether or not you are in your room, or it may be only a result of poor telephone service.

- Be particularly cautious in your relations with guides, interpreters, and travel agency personnel as these people are often used by intelligence services.

- You may be placed under physical surveillance as you travel either on foot or by vehicle. You may suspect you are being observed when actually you are not. In either event, the best tactic is to ignore it. Intelligence agents observe visitors at various times on a spot-check basis for no apparent reason. On the other hand, they may be collecting detailed data concerning your activities in preparation for a more direct intelligence approach. Do not attempt to lose the surveillance. If you are actually being followed for intelligence objectives, you will be covered by a team of several agents and your evasion attempts will only make you more suspicious.

- You probably will be allowed to take photographs with your personal camera, but be careful not to photograph restricted areas. You should refrain from taking photographs of aircraft, military and police installations or personnel, industrial structures, harbor, rail and airport facilities and border areas. Some countries also resent your photographing items which put them in a bad light such as slum areas, public drunks, scenes of civil disorder or public disturbances. If you do take such photographs your film (and camera) may be confiscated.

- Be particularly cautious in approaches which may be made offering social companionship, especially of a sexual nature. Many of these persons are plants of intelligence services and will offer themselves to you for the purpose of getting you in a compromising situation which will be followed by a blackmail threat to force your cooperation in intelligence activities. Under no circumstance should you seek or accept this kind of social companionship in a criteria country. The intelligence services are fully aware of the possibilities inherent in human frailties, and will capitalize immediately upon any indication of immoral or indiscreet behavior of American travelers. Even when failing to detect a vulnerability, agents have attempted entrapment of innocent travelers. For this reason, you should maintain the highest level of personal behavior at all times. Avoid long walks at night alone and always try to be in the company of someone you can trust. Be especially careful to stay well within your capacity for alcohol so as not to weaken your defenses, lose your self-control or impair your judgement.

- Do not accept from anyone (including friends, relatives or professional contacts) letters, photographs, packages or any other material to be smuggled out of the country or carried in your effects when you depart. Be firm in your denials in these matters as such requests may be acts of intelligence provocation to entrap you.

- Bear in mind that there are many political, cultural and legal differences between the U.S. and criteria countries. Actions which are innocent or, at worst, carry wrist slapping penalties in the U.S., are often considered serious offenses against the law in other societies. Persons violating the law, even

unknowingly, run the risk of arrest or expulsion. Do not, for instance, take souvenirs from hotels or institutions however insignificant in value they may appear.

- Do not engage in any private currency transactions with individual citizens. Do not try to sell or trade any personal items such as clothing which you have brought into the country or purchase bargains from street peddlers or other questionable vendors. Do not engage in blackmarket activities. Many countries have laws governing exportation of art work and historic relics. Be familiar with these laws if you intend to purchase such items and make these purchases only at official establishments.

- Should you be detained or arrested for any reason by police or other officials of these countries, be cooperative but insist promptly, politely and repeatedly if necessary, that the U.S. Embassy or Consulate be notified. Do not make any statements or sign any documents you do not fully understand until you have had an opportunity to confer with an embassy representative. You may possibly be accused of having some connection with an American intelligence service or of having accepted an assignment by such service to be carried out in the host country. You should make no admission whatsoever indicating you have ever had any dealings under any circumstances with any U.S. intelligence agency.

- Mail which you receive or transmit may be subject to censorship. In all mail you write prior to, during, or after your visit, make no reference to classified information or reveal information of possible value to a foreign intelligence service. Be careful when writing to or about relatives or friends in these countries as they may become targets for investigation or exploitation.

- Immediately report to the U.S. Embassy or Consulate and your CSO (during the CI debriefing) any attempts by representatives of criteria countries to:

Establish a personal or professional relationship.

Obtain information through monetary payments, bribery, observation, collection of documents, or by personal contact.

Coerce personnel by blackmail, threats against or promises of assistance to relatives living under their control.

Exploit discontented personnel or those with personal difficulties.

Intimidate, harass, entrap, discredit, search, spy on, or recruit personnel.

Induce personnel to defect or induce those who have fled from another country to redefect.

Above are some of the pitfalls that may POSSIBLY befall an American traveler. If you respect local laws and customs, are honest in your dealings and behave discreetly, you PROBABLY will not be entrapped by a foreign intelligence service and you PROBABLY will not have any problems. Have a good trip and come home safely.

EXHIBIT 3-6

COUNTERINTELLIGENCE (CI) AWARENESS DEBRIEFING

Now that you have returned from your trip to a criteria country (or a meeting), it is necessary that you be debriefed. You now have the opportunity to report any incident, no matter how insignificant it may have seemed. Specifically, we are interested in any actions by representatives of criteria countries that attempted to:

- Establish a personal or professional relationship.
- Obtain information through monetary payments, bribery, observation, collection of documents, or by personal contact.
- Coerce personnel by blackmail, threats against or promises of assistance to relatives living under their control.
- Exploit discontented personnel or those with personal difficulties.
- Intimidate, harass, entrap, discredit, search, spy on, or recruit personnel.
- Induce personnel to defect or induce those who have fled from another country to redefect.

The following are a few questions that may help you remember:

- Did anyone attempt to ask questions about your place and nature of your employment, background, hobbies, cultural and sports interests, travel desires, or other personal preferences?
- Did you receive any invitations to dinner, cocktail parties or recreational activities?
- Did anyone attempt to offer you social or sexual companionship?
- Did anyone attempt to offer to assist you in obtaining visas, export permits, licenses, etc.?
- Did anyone attempt to give you letters, packages, etc. to be delivered to someone else?
- Was there any evidence that you may have been followed?
- Did you find any evidence of listening or recording devices in your hotel room?
- Did you find any evidence of your luggage or hotel room being searched?
- Did any suspicious persons telephone you or knock on your door?
- Can you think of anything else that may be important?

If you answered yes to any of these questions, you will be required to provide a detailed narrative of the incident via the reporting procedures outlined in Chapter 2 of COMDTINST M5510.21, Information Security Program. Appropriately trained security and/or investigative personnel will take it from there.

Foreign intelligence services pose a very serious threat to our national security. It is through your understanding and accepting your responsibility to report such incidents that we, together, can thwart potential foreign intelligence efforts.

EXHIBIT 3-7

TRANSFER BRIEFING

Now that you are transferring, you are no longer authorized access to classified information at this unit. **ALL** classified material in your custody must be returned at this time.

Your security clearance has been administratively withdrawn without prejudice. If access is required at your next unit, your eligibility will be reviewed and a clearance will be requested as necessary. (NOTE: At this time, explain the individual's current clearance eligibility and what they need to maintain or upgrade that eligibility).

You must never divulge classified information, orally or in writing, to any unauthorized person or agency.

You must promptly report to Coast Guard Investigations (CGI) or the nearest Coast Guard unit, any attempt by an unauthorized person to solicit classified information from you during your transfer period.

You remain subject to the espionage laws and criminal codes applicable to the unauthorized disclosure of classified information, as explained in the Classified Information Nondisclosure Agreement (SF 312), which you signed when you were granted access.

NOTE: Attached is an optional Security Outbrief Questionnaire that may be given to the individual to voice their opinions and concerns regarding security. The questionnaire should be retained by security personnel to aid in identifying and evaluating strengths and weaknesses in the Coast Guard Security Program.

SECURITY OUTBRIEF QUESTIONNAIRE

1. What was the single-most security hazard you observed at this unit? (e.g., personnel taking classified material home to work on, unauthorized people in spaces, misuse or theft of government property, etc.) _____

2. How would you fix the problem? _____

3. Did you receive security training when you first reported here?
Yes _____ No _____ How long ago? _____
4. Did you receive periodic security training?
Yes _____ No _____ About how often? _____
5. Was the training worth your time? Yes _____ No _____
6. If training was not adequate, what should be improved? _____

7. On a scale of 1 (the lowest) to 10 (the highest), how would you rate the security awareness and practices of your co-workers? _____
8. What are the major strengths of the Coast Guard Security Program? _____

9. What are the major weaknesses of the Coast Guard Security Program? _____

10. Any other comments or suggestions? _____

THANKS FOR TAKING THE TIME TO COMPLETE THIS SURVEY!

EXHIBIT 3-8

FINAL TERMINATION BRIEFING

Now that you are no longer authorized access to classified information, we need to discuss your future security responsibilities. But first, ALL classified material in your custody must be returned at this time.

Termination of your access to classified information now does not terminate your future responsibility to protect that classified information to which you have had access. You must never divulge classified information, orally or in writing, to any unauthorized person or agency. If you ever prepare a lecture, write an article, etc., that you believe contains classified information, you are encouraged to submit the material for review to Commandant (G-OIS-2).

You must promptly report to the Federal Bureau of Investigation (FBI) or Coast Guard Investigations (CGI) any attempt by an unauthorized person to solicit classified information from you.

You remain subject to the espionage laws and criminal codes applicable to the unauthorized disclosure of classified information, as explained in the Classified Information Nondisclosure Agreement (SF 312), which you signed when you were granted access.

When you have completed this briefing, you will be asked to sign the Personnel Security Record (CG 5274) (for military) or the Security Termination Statement (DOT 1600.10) (for civilians). Read them. By signing these statements, you verify that you have received a briefing; returned all classified material in your possession; and you understand your future security responsibilities under the law.

CHAPTER 4. SECURITY TRAINING COURSES

A. Purpose. The purpose of training is to develop specific skills or capabilities which an individual will regularly use in the accomplishment of a task. This chapter prescribes the required training courses for area and district security managers (SECMGRs) assigned to the Coast Guard Security Program. Other suggested courses of instruction are also included for information purposes.

B. Priority Levels.

1. Commandant (G-PRF) has established the following priority designations and definitions for training:
 - (a) PRIORITY 1 - Essential to mission accomplishment or program objectives, which, if not provided, will have a major adverse impact on mission accomplishment or achievement of program objectives.
 - (b) PRIORITY 2 - Directly related to mission accomplishment or program objectives and should result in improvement, which, if not provided, will have a minor adverse impact on mission accomplishment or achievement of program objectives.
 - (c) PRIORITY 3 - Indirectly related to mission accomplishment or program objectives, such as to enhance overall ability of Coast Guard personnel to perform better subsequent assignments. If not provided, will have little negative impact on mission accomplishment or achievement of program objectives.
2. Exhibit 4-1 provides a list of security training courses, which have been audited and priority ranked in accordance with paragraph 4-B-1 above.

C. Area and District Security Manager (SECMGR) Training.

1. Prior to being certified by the issuance of Coast Guard security credentials and badges by Commandant (G-OIS-2), area and district SECMGRs shall complete all Priority 1 training listed in Exhibit 4-1. Priority 2 and Priority 3 training shall be completed as time and funds permit.
2. A Request, Authorization, Agreement, and Certification of Training (SF 182) shall be completed and forwarded to Commandant (G-OIS-2) for funding, quotas and scheduling.

D. Additional Training.

1. Exhibit 4-2 lists a sampling of other security related training courses that may be of benefit to Command

Security Officers (CSOs), Classified Material Control Officers (CMCOs), and other personnel involved in the security program.

2. Headquarters funding is not normally available for these courses. An SF 182 shall be completed and forwarded directly to the vendor/sponsor, unless otherwise specified in paragraph 4-D-3 below.
3. Quotas for the Department of Defense Security Institute, the Federal Law Enforcement Training Center, and the National Security Agency/Central Security Service are controlled by Commandant (G-OIS-2). An SF 182 for these training centers shall be completed and forwarded to Commandant (G-OIS-2).
4. Local colleges and universities also offers courses and degrees in security management and administration.

EXHIBIT 4-1

SECURITY MANAGER TRAINING

Listed below is security training required for area and district security managers (SECMGRs). These courses have been priority ranked in accordance with prescribed standards.

PRIORITY 1

TITLE: **DOD SECURITY SPECIALIST**
LOCATION: Department of Defense Security Institute,
Richmond, VA
LENGTH: 3 weeks
DESCRIPTION: Examines information, physical, industrial,
personnel, computer, communications, education and
training, and operations security programs through
discussion, study, and exercises in security
management, inspections and oversight.

TITLE: **SECURITY BRIEFERS**
LOCATION: Department of Defense Security Institute,
Richmond, VA
LENGTH: 3 days
DESCRIPTION: Students learn how to prepare a briefing plan, how
to present the briefing, how to design and use
briefing aids, and how to evaluate the
effectiveness of an oral briefing.

TITLE: **MANAGEMENT OF INTRUSION DETECTION SYSTEMS**
LOCATION: Norfolk Naval Shipyard Physical Security Training
Center, Portsmouth, VA
LENGTH: 1 week
DESCRIPTION: Provides broad but extensive information on
commercial integrated intrusion detection systems,
including system design, cost analysis, operational
theory, installation methods, maintenance
practices, and countermeasures of interior/exterior
intrusion detection systems.

TITLE: **OPERATIONS SECURITY FUNDAMENTALS**
LOCATION: National Security Agency, Fort Meade, MD
LENGTH: 2 days
DESCRIPTION: Provides fundamentals of Operations Security and
its application to various activities and
operations, planning, surveys, programs and
responsibilities.

TITLE: **OPERATIONS SECURITY PRACTITIONERS**
LOCATION: National Security Agency, Fort Meade, MD
LENGTH: 1 week
DESCRIPTION: Provides knowledge and skills required to perform
Operations Security planning and management
functions. Focuses on surveys and assessments,
planning and program development.

PRIORITY 2

TITLE: **CRIME AND LOSS PREVENTION PRACTICE**
LOCATION: National Crime Prevention Institute, Louisville, KY
LENGTH: 1 week
DESCRIPTION: Provides a practical foundation for physical and procedural security. Students learn how to identify crime hazards by conducting security surveys to reduce the risks of criminal events.

TITLE: **SECURITY FORCE CONTRACTING**
LOCATION: GSA Interagency Training Center, Arlington, VA
LENGTH: 3 days
DESCRIPTION: Students gain an understanding of the contracting cycle, learn how to develop security contracts and effective work statements, and ensure quality performance.

TITLE: **GOVERNMENT SECURITY CONTAINERS**
LOCATION: Mosler National Education Center, Hamilton, OH
LENGTH: 1 week
DESCRIPTION: Provides an overview of GSA security devices, including all aspects of modern security files and locks. Specifications for security containers, files, locks and vault doors are discussed along with construction details and basic operations.

TITLE: **COMBATTING TERRORISM ON MILITARY INSTALLATIONS**
LOCATION: US Army Military Police School, Fort McClellan, AL
LENGTH: 1 week
DESCRIPTION: Discusses terrorist organizations, strategies, tactics and capabilities, current threats, legal considerations, emergency operation centers, physical security, personnel protection and crisis management.

TITLE: **SECURITY, SUITABILITY, ADJUDICATION & AWARENESS**
LOCATION: Office of Personnel Management, Washington, DC
LENGTH: 4 days
DESCRIPTION: Provides information on disqualifying factors, case processing, position sensitivity, adjudications, due process, appeals, records and safeguards.

TITLE: **CLASSIFICATION MANAGEMENT**
LOCATION: Department of Defense Security Institute, Richmond, VA
LENGTH: 1 week
DESCRIPTION: Provides core concepts and policies of classification management, terminology, original classification decision process, classification guidance, problems in the derivative classification process, impact on the industrial security program, and reevaluation of classification.

PRIORITY 3

TITLE: PERSONAL SECURITY IN THE WORKPLACE
LOCATION: GSA Interagency Training Center, Arlington, VA
LENGTH: 1 week
DESCRIPTION: Students study the philosophies of crime prevention programs for the workplace, and the ways employees and managers can work together to reduce crime.

TITLE: ADVANCED PHYSICAL SECURITY
LOCATION: Federal Law Enforcement Training Center, Glynco, GA
LENGTH: 8 days
DESCRIPTION: Provides conceptual frameworks, vulnerability assessments, familiarization with hardware and procedures, exercises and report presentation. Subject matter includes threat analysis, risk assessment, intrusion detection systems, access control, security design, legal considerations, guard force issues, lighting, locking devices, CCTV, and physical security surveys.

TITLE: LOCKS AND LOCKING DEVICES 1
LOCATION: National Intelligence Academy, Ft. Lauderdale, FL
LENGTH: 1 week
DESCRIPTION: Provides students with an in-depth knowledge and understanding of locks and locking devices and the skills necessary to neutralize such locks and devices. Subject matter includes warded locks, disc tumbler locks, pin tumbler locks, lever locks, tool making, picking, and by-pass techniques.

EXHIBIT 4-2

SECURITY RELATED TRAINING

Listed below is a compilation of other suggested security training; it is not a complete list. The Coast Guard has not evaluated each course and makes no endorsement as to quality or suitability.

**Department of Defense Security Institute
Defense General Supply Center
8000 Jefferson Davis Highway
Richmond, VA 23297-5091
(804) 279-4891**

Security Specialist	3 weeks
Security Briefers	3 days
Train-the-Trainer	5 days
Information Security Orientation	3 days
Information Security Management	2 weeks
Classification Management	1 week
Security for Special Programs	2 weeks
Basic Personnel Security Investigations	2 weeks
Personnel Security Adjudications	2 weeks
Advanced Personnel Security Adjudications	2 weeks
Personnel Security Interview	1 week
Personnel Security Management	2 weeks
User Agency Inspector	8 days
Industrial Security Specialist	6 weeks
Industrial Security Executive Seminar	1 week

CORRESPONDENCE COURSES

Personnel Security Adjudications
Physical Security
Automated Data Processing (ADP) Concepts and Terms
Structures of Industrial Security
Basic Industrial Security for User Agency Personnel
Essentials of Industrial Security Management
Protecting Secret and Confidential Documents

**National Security Agency/Central Security Service
Fort George G. Meade, MD 20755-6000
(410) 859-6166**

Operations Security Fundamentals	2 days
Operations Security Practitioners	1 week
Information Security Cadre Course	1 week
National Computer Security Course	1 week

**Department of Treasury
Federal Law Enforcement Training Center
Quota Scheduler, Building #94
Glynco, GA 31524
(912) 267-2421**

Physical Security Managers	3.5 days
Advanced Physical Security	8 days

Anti-terrorism Management	3 days
Anti-terrorism Contingency Planning	3 days
Police Training Program	8 weeks
Officer Safety and Survival	2 weeks

U.S. Coast Guard Institute
P.O. Substation 18
Oklahoma City, OK 73169-6999
(405) 686-4388

CORRESPONDENCE COURSE

Security of Classified Information

GSA Interagency Training Center
PO Box 15608
Arlington, VA 22215-0608
(703) 557-0986

Physical Security	1 week
Security Evaluation Procedures	3 days
Security Force Contracting	3 days
Personal Security in the Workplace	1 week
Terrorism	3 days
Security Systems Technology	3 days
Risk Assessment/Contingency Planning	1 week
Computer Security	1 week
Computer Security Awareness	1 day

Department of Navy
Norfolk Naval Shipyard, Code 1120
Physical Security Training Center
Portsmouth, VA 23709-5000
(804) 396-3007

Management of Intrusion Detection Systems	1 week
Operations and Maintenance of Intrusion Detection Systems	8 days

Department of Navy
Naval Technical Training Center Detachment
1500 Shaw Drive, Lackland AFB
San Antonio, TX 78236-5418
(512) 671-3263/3203

Navy Security Officer	3 weeks
Navy Security Guard	6 weeks

Department of Navy
Naval Criminal Investigative Service
MTT LANT
2600 Tarawa Court
Norfolk, VA 23521-3227
(804) 464-8925

MTT PAC
PO Box 80397
San Diego, CA 92138-0397
(619) 524-6277

Navy Physical Security & Law Enforcement Supervisor 4.5 days

Department of Air Force
Security Police Academy
343rd TTS/CCQA
1350 Scott Drive, Suite 1, Lackland AFB
San Antonio, TX 78236-5429
(512) 671-2801

Base and Installation Security System	2 weeks
Security Supervisor	3 weeks
Law Enforcement Supervisor	3 weeks
Tactics for Emergency Service Teams	2.5 weeks
Security Police Officer Course	6 weeks
Security Specialist	5.5 weeks
Traffic Management and Accident Investigation	3.5 weeks

Department of Air Force/SIA/ATS
226 Duncan Avenue, Suite 2100, Bolling AFB
Washington, DC 20332-0001
(202) 767-5254/5266

Advanced Security Vulnerabilities Investigations	2 weeks
--	---------

Department of Army/CML & MPCEN & FM
ATTN: ATZN-MP-TRT/004
Fort McClellan, AL 36205-5030
(205) 848-3457

Conventional Physical Security/Crime Prevention	2 weeks
Special Ammunition Security	2 weeks
Combatting Terrorism on Military Installations	1 week
Special Reaction Team	2 weeks

Department of Army/CEMRO-ED-ST
U.S. Army Engineer District, Omaha
215 North 17th Street
Omaha, NE 68102-4978
(402) 221-3072

Security Engineering (Protective Design)	4 days
--	--------

Department of Army
The Army Institute for Professional Development
U.S. Army Training Support Center
Newport News, VA 23628-0001
(804) 878-2169

CORRESPONDENCE COURSES

Classified Document Procedures
Handling Classified Documents
Safeguarding Defense Information
Personnel Security Program
Operations Security
Security Services
Automated Data Processing System Security
Threat Assessment
Countermeasures Development
Physical Security Planning

Physical Security
 Area Security
 Material Control
 Civil Disturbance Planning
 Law Enforcement Operations
 Military Police Control
 Economic Crimes
 Communications Security

Department of Energy
 Central Training Academy
 PO Box 18041
 Albuquerque, NM 87185
 (505) 845-5170

Introduction to Physical Security Systems	1 week
Sensors Systems Course I	1 week
Sensors Systems Course II	1 week
Explosive Threat Recognition, Prevention & Response	1 week
Special Response Team	4 weeks

Department of State
 Diplomatic Security Training Center
 DS/PLD/TSD, SA-11
 Washington, DC 20522-1003
 (703) 204-6100

Lock Training	Varies
---------------	--------

Central Intelligence Agency/OS-SED
 1517 West Branch Drive
 McLean, VA 22102
 (703) 506-7235

Basic Combination Locks	1 day
Domestic Security Equipment	3 days
Introduction to Physical Security	8 days

National Intelligence Academy
 1300-1400 N.W. 62nd Street
 Fort Lauderdale, FL 33309
 (305) 776-5500

Locks and Locking Devices I	1 week
Locks and Locking Devices II	1 week

Defense Intelligence College
 Washington, DC 20340-5485
 (202) 373-3292

Counter-terrorism Analysis	2 weeks
Advanced Counter-terrorism Analysis	1 week
Counter-terrorism Perspectives for Senior Managers	3 days
Multidiscipline Counterintelligence Analyst	2 weeks

DOD Polygraph Institute
Building 3195
ATTN: ATZN-DPI
Fort McClellan, AL 36205
(205) 848-3336

Espionage	1 week
Technological Impact on Espionage	1 week

Office of Personnel Management
Office of Federal Investigations
600 E. Street N.W., Room 800
Washington, DC 20044
(202) 376-3800

Security, Suitability, Adjudication & Awareness	4 days
Processing Investigative Forms	1 day

Hampton Roads Regional Academy of Criminal Justice
1300 Thomas Street
Hampton, VA 23669
(804) 722-2848

Basic Crime Prevention	1 week
------------------------	--------

National Crime Prevention Institute
University of Louisville, Shelby Campus
Burhans Hall, Room 134
Louisville, KY 40292
(502) 588-6987

Advanced Physical Security	1 week
Advanced Alarms and Electronic Security	1 week
Advanced Locks and Locking Systems	1 week
Crime and Loss Prevention Practice	1 week
Crime and Loss Prevention Technology & Programming	2 weeks
Crime and Loss Prevention Theory, Practice and Management	3 weeks
Crime and Loss Prevention Management	1 week
Crime Prevention Administration	1 day
Crime Prevention Through Environmental Design	2 weeks

Florida Crime Prevention Institute
Attorney General's Office/The Capitol
Tallahassee, FL 32399-1050
(904) 487-3712

Crime Prevention Program Development	1 week
Convenience Store Security	3 days
Residential Security	1 week
Crime Prevention Practitioner Update/Technology	3 days
Commercial Security	1 week

Institute of Criminal Justice Studies
Southwest Texas State University
West Campus-Canyon Hall
San Marcos, TX 78666-4610
(512) 245-3031

Introduction to Crime Prevention	4 days
Basic Crime Prevention for Practitioners	2 weeks
Crime Stoppers Public Speaking	1 week
Non-Violent Physical Restraint	2 days

University of Delaware
2800 Pennsylvania Avenue
Wilmington, DE 19806
(302) 573-4440

Managing the Small Police Department	3 days
Field Officer Safety Procedures	2 days
First-Line Police Supervisory Practices	3 days
Managing Department Training Operations	3 days
Use of Supervisory Principles within Communication Centers	2 days
Perspectives on DOD Security Force Management	2 days
Crisis Management & Contingency Planning	2 days
Intrusion Detection Systems: Operation and Application	2 days
Application of Physical Security Systems	2 days
Premises Survey and Security Planning	2 days

Mosler National Education Center
8509 Berk Boulevard
Hamilton, OH 45012
(513) 870-1049

Government Security Containers	1 week
--------------------------------	--------

Lockmasters Professional School
5085 Danville Road
Nicholasville, KY 40356
(800) 654-0637

Government Security Container	1 week
Professional Locksmithing	2 weeks
Safe Deposit Lever Lock Servicing	3 days
Safe Lock Servicing	4 days
Basic Safe Penetration	3 days
Combination Lock Manipulation	4 days
Time Lock Technology	1 week

CORRESPONDENCE COURSES

Safe Lock Servicing
Combination Lock Manipulation
Safe Deposit Lock Servicing

American Society for Industrial Security
1655 North Fort Myer Drive, Suite 1200
Arlington, VA 22209
(703) 522-5800

Assets Protection I	1 week
Assets Protection II	1 week
Assets Protection III	1 week
Telecommunications Security	3 days
Securing Your Networks	3 days
Physical Security Technology and Applications	3 days
Facility Security Design	3 days
White Collar Crime	2 days
Educational Institutions Security	2 days
Advanced Guard Force Management	2 days

Quintilian Institute Services
5001A Lee Highway, #101
Arlington, VA 22207
(703) 525-7525

Safes, Vaults and Security Containers	2 days
Combination Lock Service	2 day
Defense Against Methods of Entry	2 days
Advanced Safe Procedures	2 days
Electronic Locks and Access Control	2 days
Drugs and Narco Terrorism	3 days
SCIF Construction and Accreditation	5 days

SECURITY RELATED REFERENCES

COMDTINST M2000.3 (series), Telecommunications Manual (TCM)

COMDTINST CM2241.1 (series), Shore Facilities Design...For Secure Electrical Info Processing Systems

COMDTINST M2600.1 (series), Communications Tactical (COMTAC) Publication Index

COMDTINST M4500.5 (series), Property Management Manual

COMDTINST M5100.47 (series), Safety and Environmental Health Manual

COMDTINST M5212.12 (series), Paperwork Management Manual

COMDTINST 5220.5 (series), Investigative Assistance

COMDTINST M5260.2 (series), Privacy (Coast Guard) and Freedom of Information Acts Manual

COMDTINST M5500.13 (series), Automated Information Systems (AIS) Security Manual

COMDTINST M5500.17 (series), Standard Workstation Security Handbook

COMDTINST 5510.18, Security Classification Guide for International Movements of Controlled Substances Information

COMDTINST M5500.19 (series), U.S. Coast Guard North Atlantic Treaty Organization (NATO) Security Manual

COMDTINST M5510.21 (series), Coast Guard Information Security Program

COMDTINST M5520.12 (series), Coast Guard Personnel Security Program

COMDTINST M5527.1 (series), Investigations Manual

COMDTINST M5530.1 (series), Physical Security Program

COMDTINST M5830.1 (series), Administrative Investigations Manual

COMDTINST M6000.1 (series), Medical Manual

COMDTINST M8000.2 (series), Ordinance Manual

COMDTINST M8370.11 (series), Small Arms Manual

COMDTINST 16246.1 (series), Handling Classified Material in Criminal Prosecutions

Encl (1) to COMDTINST M5528.1

DOT Order 1600.26 (series), Department of Transportation Physical Security Program

DOT Order 1630.2 (series), Personnel Security Program Handbook

DOT Order 1640.4 (series), Classification, Declassification and Control of National Security Information

DOT Order 1650.1 (series), Technical Security Countermeasures Program

DoD 5220.22-R (series), Industrial Security Regulation

DoD 5220.22-M (series), Industrial Security Manual for Safeguarding Classified Information

CMS-1 (series), Communications Security Material System (CMS) Manual

DIAM 50-3, Physical Security Standards for Construction of Sensitive Compartmented Information Facilities

NSDD 298, National Operations Security Program

Executive Order 10450, Security Requirements for Government Employees

Executive Order 10865, Safeguarding Classified Information Within Industry

Executive Order 12356, National Security Information

Executive Order 12829, National Industrial Security Program

SECURITY RELATED FORMS

Listed below are all security related forms used in the Coast Guard Security Program. COMDTINST M5213.6 (series), Catalog of Forms, provides further requisitioning information.

CG-3308A	Certificate of Compliance - Private Motor Vehicle Registration
CG-4764	Security Violation Notice
CG-4764A	Top Secret Disclosure Record
CG-4801	Coast Guard Registration Decal
CG-4819	Classified Document Control Log
CG-5044	Authority for Release of Information for Background Investigation
CG-5274	Personnel Security Record
CG-5439	Coast Guard Security ID Badge - TOP SECRET (Orange)
CG-5439A	Coast Guard Security ID Badge - TOP SECRET (Sensitive Compartmented Information)
CG-5439B	Coast Guard Security ID Badge - SECRET (Red)
CG-5439C	Coast Guard Security ID Badge - CONFIDENTIAL (Blue)
CG-5439D	Coast Guard Security ID Badge - UNCLEARED (Green)
CG-5439E	Coast Guard Security ID Badge - VISITOR (All Colors)
CG-5448	Coast Guard Security Badge Record
CG-9733	Document Receipt
DD-254	DoD Contract Security Classification Specification
DD-398	Personnel Security Questionnaire (PSQ)
DD-398-2	National Agency Questionnaire (NAQ)
DD-2501	Courier Authorization
SF-85	Questionnaire for Non-Sensitive Positions
SF-85P	Questionnaire for Public Trust Positions
SF-86	Questionnaire for Sensitive Positions
SF-87	Fingerprint Chart
SF-312	Classified Non-Disclosure Agreement

Encl(2) to COMDTINST M5528.1

SF-700	Security Container Information (envelope)
SF-701	Activity Security Checklist
SF-702	Security Container Check Sheet
SF-703	TOP SECRET Cover Sheet
SF-704	SECRET Cover Sheet
SF-705	CONFIDENTIAL Cover Sheet
SF-706	TOP SECRET Medium Label (Orange)
SF-707	SECRET Medium Label (Burgundy)
SF-708	CONFIDENTIAL Medium Label (Blue)
SF-709	Classified Medium Label (Purple)
SF-710	Unclassified Medium Label (Green)
SF-711	Data Descriptor Label (White)
OPNAV 5510/413	Personnel Security Action Request
OPNAV 5510/21	Security Container Record Form
OPNAV 5521/27	Visit Request Form
DOT-1600.8	Personnel Security Action Request
DOT-1600.10	Security Termination Statement
DOE F 5631.18	Security Termination Statement
DOE F 5631.29	Security Acknowledgement
FD-258	Applicant Fingerprint Form

INDEX

- A -

PAGE(S)

Access Briefing.....3-1, Exhibit 3-3
Administrative Security Discrepancies.....Exhibit 3-3
Aids, Teaching.....2-6
Airport Safety.....Exhibit 3-4
Annual Refresher Briefing.....3-2
Arrival Briefing.....3-1, Exhibit 3-2
Associations.. ..2-2, Exhibit 2-1
Audiovisuals.....2-2, Exhibit 2-3
Awareness, defined.....1-1

- B -

Books.....Exhibit 2-4
Briefings
 Access.....3-1, Exhibit 3-3
 Annual Refresher.....3-2
 Arrival.....3-1, Exhibit 3-2
 Counterintelligence Awareness.....3-1, Exhibit 3-5
 Final Termination.....3-2, Exhibit 3-8
 Foreign Travel.....3-1, Exhibit 3-4
 Record of.....3-3
 Transfer.....3-2, Exhibit 3-7

- C -

Classification
 Derivative.....Exhibit 3-3
 Original.....Exhibit 3-3
Command Security Officer Responsibility.....3-1
Compromises.....Exhibit 3-3
Consciousness, Security.....1-3
Consulate, U.S.....Exhibit 3-4, Exhibit 3-5
Counterintelligence Awareness Briefing.....3-1, Exhibit 3-5
Counterintelligence Awareness Debriefing.....3-2, Exhibit 3-6
Courses
 Correspondence.....Exhibit 4-2
 Training.....4-1, Exhibit 4-1, Exhibit 4-2
Criteria Country.....3-2, Exhibit 3-5, Exhibit 3-6

- D -

Debriefing, Counterintelligence Awareness.....3-2, Exhibit 3-6
Derivative Classification.....Exhibit 3-3

- E -

Education, defined.....1-1
Embassy, U.S.....Exhibit 3-4, Exhibit 3-5

- F -

Final Termination Briefing.....3-2, Exhibit 3-8

Foreign Intelligence Threat.....Exhibit 3-3
Foreign Travel Briefing.....3-1, Exhibit 3-4
Forms.....Enclosure (2)

- G -

- H -

Hostage Survival.....Exhibit 3-4
Hotel Safety.....Exhibit 3-4

- I -

Implementation, Program.....2-1
Information Security.....Exhibit 3-2

- J -

- K -

- L -

Learning.....2-4
Literature.....2-3, Exhibit 2-4
Loss Prevention.....Exhibit 3-2

- M -

Marking.....Exhibit 3-3

- N -

Newsletters.....2-3
Nondisclosure Agreement.....Exhibit 3-3, Exhibit 3-7, Exhibit 3-8

- O -

Objectives, SATE.....1-1
Operations Security.....Exhibit 3-2
Organizations.....2-2, Exhibit 2-1
Original Classification.....Exhibit 3-3
Outbrief Questionnaire.....Exhibit 3-7

- P -

Performance.....1-4
Personal Recognition.....1-3
Personnel Security.....Exhibit 3-2
Posters.....2-2, Exhibit 2-2
Presentation Methods.....2-5
Priority Levels.....4-1, Exhibit 4-1
Program Implementation.....2-1
Publications.....Exhibit 2-4

- Q -

Questionnaire.....Exhibit 3-7
Quotas.....4-2

- R -

Recognition.....	1-3
References.....	Enclosure (1)
Refresher Briefing, Annual.....	3-2
Responsibilities	
Command Security Officer.....	3-1
Commandant.....	1-2
Individual.....	1-2
Resources.....	2-2

- S -

Safeguarding.....	Exhibit 3-3
Security Awareness Day/Week/Month.....	2-3
Security Consciousness.....	1-3
Schedule of Briefings.....	Exhibit 3-1
Sources	
Audiovisuals.....	Exhibit 2-3
Literature.....	Exhibit 2-4
Organizations/Associations.....	Exhibit 2-1
Posters.....	Exhibit 2-2
Publications.....	Exhibit 2-4

- T -

Teaching Aids.....	2-6
Termination Briefing.....	3-2, Exhibit 3-8
Tests.....	2-6, Exhibit 2-5
Threat, Foreign Intelligence.....	Exhibit 3-3
Training Courses.....	4-1, Exhibit 4-1, Exhibit 4-2
Training, defined.....	1-1
Transfer Briefing.....	3-2, Exhibit 3-7
Travel, Foreign.....	3-1, Exhibit 3-4

- U -

U.S. Consulate.....	Exhibit 3-4, Exhibit 3-5
U.S. Embassy.....	Exhibit 3-4, Exhibit 3-5

- V -

Vehicle Security.....	Exhibit 3-4, Exhibit 3-5
-----------------------	--------------------------

- W -

- X -

- Y -

- Z -

